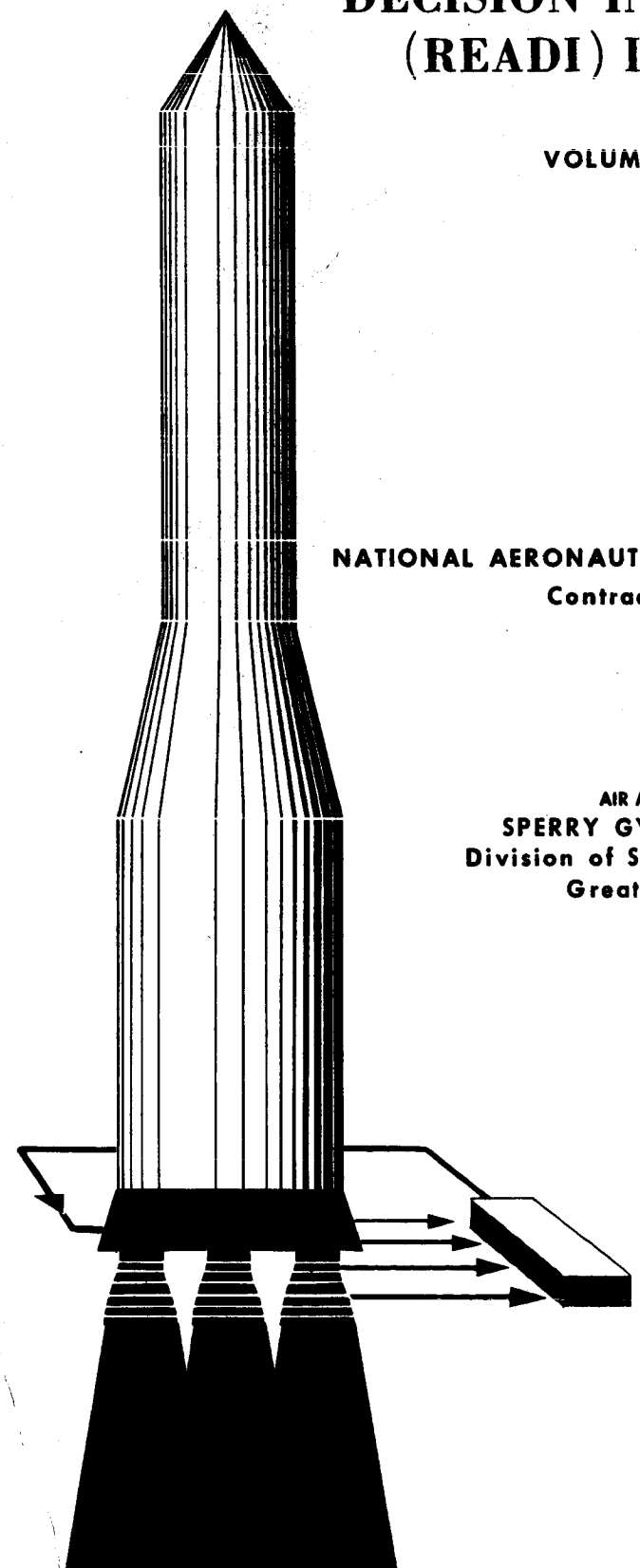
FINAL REPORT
PHASE I

ROCKET ENGINE ANALYZER AND DECISION INSTRUMENTATION (READI) INVESTIGATION

VOLUME II - APPENDICES



Prepared for
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION
Contract No. NAS 8-4003

Prepared by
AIR ARMAMENT DIVISION
SPERRY GYROSCOPE COMPANY
Division of Sperry Rand Corporation
Great Neck, New York

Sperry Report No. CA-4251-0160 Volume II

December 1962

FINAL REPORT

PHASE I

ROCKET ENGINE ANALYZER AND DECISION INSTRUMENTATION (READI) INVESTIGATION

VOLUME II - APPENDICES

Prepared for

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

Contract No. NAS 8-4003

Prepared by

AIR ARMAMENT DIVISION

SPERRY GYROSCOPE COMPANY

Division of Sperry Rand Corporation

Great Neck, New York

ENGINEERING DEPARTMENT

E.S.Joline

R.L.Smith

J.L.Keller

D.P.Blowney

P.G.Yiotis

J.Harrison

PUBLICATIONS DEPARTMENT

B.R.Maffia

Sperry Report No. CA-4251-0160 Volume II

Copy No. 01

December 1962

ABSTRACT

The rocket engine analyzer and decision instrumentation concept comprises an on-board electronic system that analyzes the condition of a rocket propulsion system and takes corrective action, either automatically or through the pilot, in order to increase the probability of mission success and safety of the crew.

This concept has been investigated to:

- determine its economic feasibility
- develop a design approach
- gain familiarization with the functional operation and equipment required for a typical system.

A philosophy of approach and detailed design and evaluation procedure are described in which the input data and assumptions are clearly identified and the calculations are performed by a digital computer.

An equipment configuration is described and special reliability techniques are discussed which will permit achieving the functional and reliability requirements as determined by the design procedure.

These design and equipment approaches have been applied to a representative mission-vehicle-engine combination. The results indicate that application of the READI concept to launch vehicles offers a substantial potential return in reduction of mission risk.

FOREWORD

This Final Report on Rocket Engine Analyzer and Decision Instrumentation has been prepared for the National Aeronautics and Space Administration by the Air Armament Division of Sperry Gyroscope Company Division of Sperry Rand Corporation, Great Neck, New York, under Contract No. NAS 8-4003.

The program was initiated by Mr. H. Burlage, Office of Liquid Rockets, NASA Headquarters, Washington, D.C., and has been under the technical cognizance of Messrs. D. Pryor and K. Chandler, P & VE, Marshall Space Flight Center, Huntsville, Ala.

Personnel from Reaction Motors Division of Thiokol Chemical Corp. who contributed to the program include W. Brewington, W. M. Bogert Jr., A. M. Brukardt and E. Tesch.

TABLE OF CONTENTS

VOLUME I - SUMMARY

TABLE OF CONTENTS (Cont.)

TABLE OF CONTENTS (Cont.)

TABLE OF CONTENTS (Cont.)

TABLE OF CONTENTS (Cont.)

LIST OF ILLUSTRATIONS

VOLUME I - SUMMARY

LIST OF ILLUSTRATIONS (Cont.)

VOLUME II - APPENDICES

LIST OF ILLUSTRATIONS (Cont)

LIST OF ILLUSTRATIONS (Cont.)

LIST OF TABLES

VOLUME I - SUMMARY

VOLUME II - APPENDICES

- - - - - - -

*After page

LIST OF TABLES (Cont)

VOLUME II - APPENDICES (Cont)

- - - - - - - -

*After page

Appendix A

READI FUNCTIONAL REQUIREMENTS

APPENDIX A

READI FUNCTIONAL REQUIREMENTS

A-1. INTRODUCTION

This appendix describes the equipment requirements for a READI system integrated into a three-stage launch vehicle. From the standpoint of equipment design the requirements presented here constitute a preliminary equipment specification. The subsequent appendices, which deal with major equipment design considerations, trade-off evaluations, and integration into the launch vehicle, deal with a system designed to meet these requirements.

The selection of engine condition identification equations and transducer inputs presented here represents one point in a system cost versus risk trade-off. Although not an optimized set of signals, the resulting READI design is representative of the complexity to be expected in a comprehensive analyzer which is used in a manned space mission.

The detailed requirements presented are for the second stage of the launch vehicle. Additional data is presented to aid in extrapolating the design to the first and third stages. The specific engine and tankage configuration is described in Appendix G. The mission for which the launch vehicle is designed is described in Appendix F.

A-2. EQUIPMENT OBJECTIVE

The READI system monitors the performance of the launch vehicle engines and initiates corrective action in case of malfunctions in order to lower the risk to crew and mission.

A. SCOPE

The READI system monitors primary signals from the rocket engines, the control pressure system, and the propellant pressurization system. Additional signals such as time-to-go and vehicle attitude rates are also required from other vehicle subsystems. All corrective actions are initiated through the rocket engines. The equipment includes transducers to monitor propulsion system signals, electronic equipment to identify the system condition and initiate corrective action, and interconnecting cabling.

B. INPUTS TO SECOND STAGE READI SYSTEM

Table A-1 lists the inputs to the system and the type of transducer to be employed. Each engine employs 26 transducers and two inputs from the engine sequencer control. Additional internal signals are generated, for instance, to serve as time reference gates in identifying engine condition (table A-2, S52).

A-3. EQUIPMENT OPERATIONS

As a general rule, the equipment operations may be divided into two parts: the processing of input transducer signals and the logical operation of forming decisions from the binary-processed input signals. Table A-2 shows the processing or signal conversion for each signal used in each identification (V) of engine condition in the system. Also shown in table A-2 is the logical operation necessary to identify the engine condition. This is given under the heading "Definition of V".

A. OUTPUT DECISIONS

The model engine has the capability of the following alternate actions in addition to no action:

- shut down
- restart
- fast shut down
- fast restart
- increase thrust (to maximum)
- decrease thrust (to normal).

For the conditions resulting from the possible failures in propulsion system (5 engines and tankage) the following list shows the programmable decisions which may be used to advantage. Note that the decisions are the actions taken singly, in combinations, and in sequence, with READI monitoring the intermediate engine condition.

1. Programmable Decisions

   D - Action Required

   1 No action

   2 Shut down subject engine

4 D2 + increase thrust on other engines

6 D4 + restart and return to normal thrust if engine is OK

7 Fast shut down + D6

11 Fast shut down and restart if engine is OK

Table A-2 also shows the decision number which should be programmed for each V which is indicated by READI.

The actions which constitute the programmed decisions are implemented by either energizing or de-energizing each of three wires which lead to each engine sequence controller. The required output logic is shown below, along with a short description of the resulting action by the engine.

Wire No.	State	Action
1	energized	Shut down
	de-energized	Restart
2	energized	Fast shut down
	de-energized	Fast restart
3	energized	Increase thrust
	de-energized	Decrease thrust

2. Resulting Action (refer to engine electrical schematic, figure G-2)

Energize Wire No. 1 - Open S5 and S7 - This de-energizes main propellant valve, tank safety valve, and gas generator bootstrap valve solenoids.

De-energize Wire No. 1 - Close S5 - This puts engine in prestart mode. Engine proceeds to start mode (close S7) either manually or automatically when satisfactory prime pressure is indicated by prime light.

Energize Wire No. 2 - Energizes solenoid L3 which causes main propellant valve to shut at maximum rate.

De-energize Wire No. 2 - De-energizes solenoid L3 permitting attempt at normal restart.

Energize Wire No. 3 - Energize motor B-1 to drive gas generator bootstrap valve to maximum stop.

De-energize Wire No. 3 - Energize motor B-I to drive to nominal flow stop.

The output decision logic for all programmable decisions for failures in engine No. 1 of a five engine state is shown in table A-3. The conditional action [0] implies that the READI system is monitoring the engine and if the condition is restored to normal, the noted action is taken.

B. PROCESSING TIME

The time which can be allotted for processing the electronic inputs is a function of allowable time from malfunction to accomplishment of corrective action and the lags in sensing and correction loop. A discussion of this problem appears in Appendix H. The allowable processing times for each identification of engine condition (V) are also found in table A-2.

C. ACCURACY OF IDENTIFICATION

Table A-2 also shows the allowable three-sigma error in each S as used in each V. The allowable errors in processing circuitry are also shown, based on currently achievable transducer accuracies. This allotment assumes a root sum square distribution of errors between the transducer and the processing circuitry.

D. FIRST AND THIRD STAGE READI DESIGN

The READI requirements in terms of number of transducers and identification are substantially the same for the third stage as the second. The significant difference is that there is only one engine in the third stage. Therefore, transducer and signal processing complexity is reduced by a factor of five. Also, actions related to increasing thrust on other engines are also eliminated.

The first stage, like the second, employs five engines. The engines are somewhat less complex, however, and require only about 12 engine condition identification equations (V equations) for the same equipment cost-risk trade-off point as used for the second stage. The number of transducers per engine is reduced from 26 to 16. In addition, the decisions involving restart are modified since the first stage engine is assumed not to have this capability.

A-4. RELIABILITY

A set of inputs, processing, and decisions is given in table A-2 for which the READI electronics must be designed. The purpose of these paragraphs is to clarify the reliability requirements of the electronics and transducers with regard to cost and mission risk.

The reliability of the system is stated in the form of false alarm and missed alarm rates per mission. This approach is related directly to the objective of the equipment, which is to initiate corrective action in case of malfunctions in order to lower the risk to crew and mission. Figure A-1 is a plot of mission risk in dollars versus failure rate, per mission. With the aid of the curves in figure A-1 an effective trade-off can be made between the cost and risk for each channel, or engine identification, and the design techniques used, such as transducer and circuit redundancy and self-check techniques.

TABLE A-1

INPUT SIGNALS TO SECOND STAGE READI SYSTEM

Input Signal Designation	
2	Pre-start Circuit Voltage
3	Fire Circuit Voltage
5	Vibration
6	Turbine Speed Sensor
9	Fire Detector
11	Oxidizer Flow (one engine)
12	Fuel Flow (one engine)
16	Igniter Prop Valve (U_2) Limit Switch (Position)
18	Fast Shut Down Valve (U_3) Limit Switch (Position)
19	Tank Safety Valve (U_4) Limit Switch (Position)
22	Mam Chamber Pressure
23	Igniter Chamber Pressure
24	Oxidizer Injector Pressure Drop
25	Fuel Injector Pressure Drop
30	Oxidizer Pump Inlet Pressure
31	Fuel Pump Inlet Pressure
32	Oxidizer Pump Discharge Pressure
33	Fuel Pump Discharge Pressure
35	Prime Valve (U_5) Outlet Pressure
44	Gas Generator Chamber Temperature
55	Fuel Injector Temperature, Mam Chamber
56	Oxidizer Injector Temperature , Mam Chamber
71	Oxidizer Temperature at Flow Meter
72	Fuel Temperature at Flow Meter

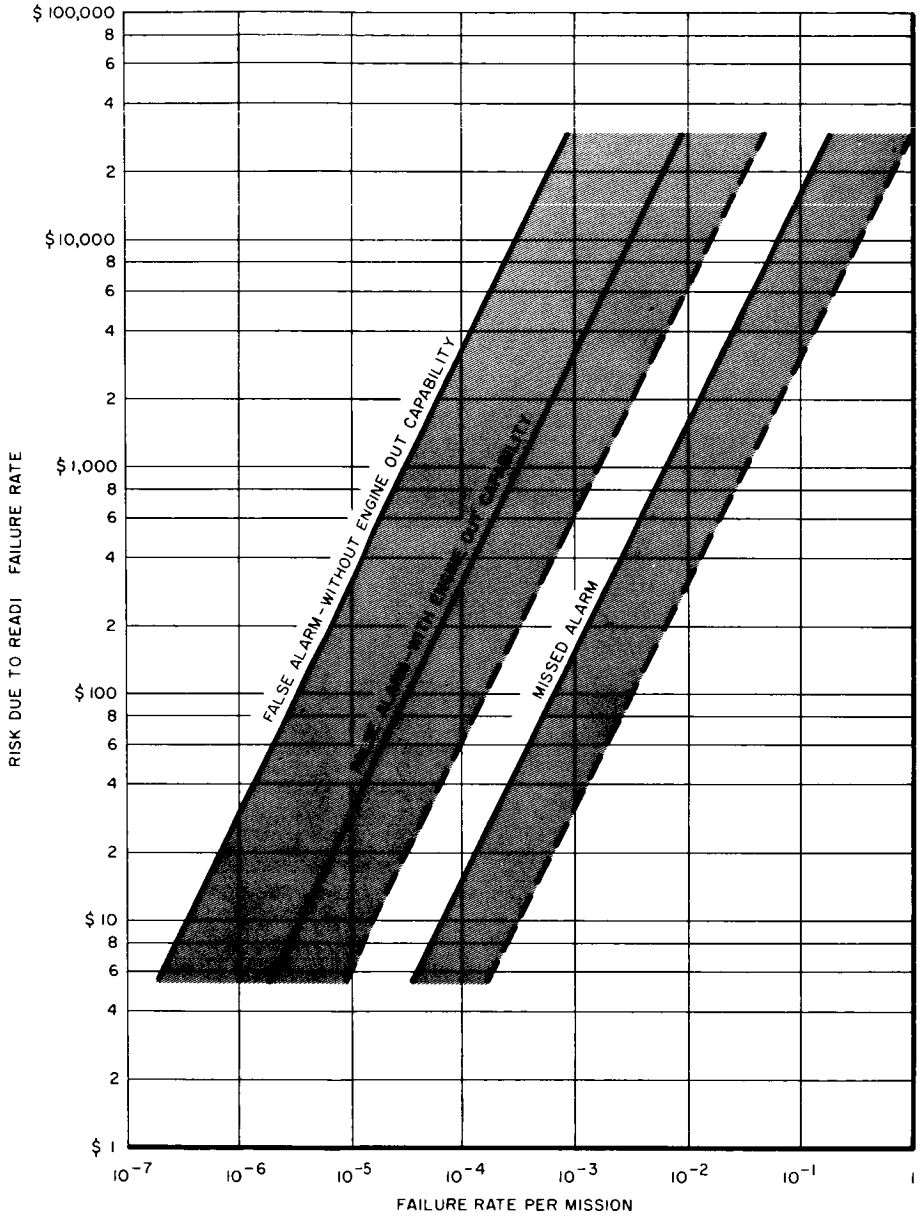


FIGURE A-1

SENSITIVITY OF RISK TO READI FAILURE RATE FOR
TYPICAL ENGINE CONDITION IDENTIFICATION CHANNEL

TABLE A-2 (Cont)

READI MODEL SYSTEM REQUIREMENTS

V	Malf. Area	Signal	Signal Processing	Definition of V (Boolean Notation)	Allowable Processing Time, msec	Allowable Error		Programmed Decision Number			
						V %	Processing Circuit %	Pre-Start	Start	Operate	Shutdown
181	18	11			500	±1	±0.7	1	1	4	1
		24	$S24 < 7.15(S11)^2(S56)X10^{-6}$	S24		±2	±1				
201	20	9.2*	$>700^{\circ}F$	S9.2	1900	±5	±2.5	2	4	4	2
211	21	44	$>1800^{\circ}F$	S44	25			1	4	4	1

Notes:

1 - ( )* READI generated signal, not a transducer input

2 - Accuracy is expressed as percent of value of S at processing reference point, except when reference is zero in which case accuracy is percent of full scale

TABLE A-2

READI MODEL SYSTEM REQUIREMENTS

V	Malf. Area	Signal	Signal Processing	Definition of V (Boolean Notation)	Allowable Processing Time, msec	Allowable Error		Programmed Decision Number			
						V %	Processing Circuit %	Pre-Start	Start	Operate	Shutdown
401	-	22	<100 psia	S22(S23)S52	25	±10	±7	2	4	4	2
		23	<100 pisa			±10	±7				
		(52)*	>2 sec			±5	±5				
402	-	9.1	>700°F	S9.1	50	±5	2.5	2	4	4	2
403	-	6.2	>40,000 rpm	S6.2 + (S6.1)(S54)	25	±3	±2.5	1	4	4	2
		6.1	>27,000 rpm			±3	±2.5				
		(54)*	>40,000 rmp/sec			±5	±5				
22	2	12	<72 lb/sec		500	±1	±0.7	1	1	4	1
		30	S30-S31 >10 psi	[(S6)(S12) + (S30 - S31)]		±5	±3				
		31				±5	±3				
		6	>32,000 rpm			±3	±2				
32	3	11	<382 lb/sec		1900	±1	±0.7	1	1	4	1
		30	S31-S30 >10 psi			±5	±3				
		31		[(S6)S11 + (S31 - S30)]		±5	±3				
		6	>32,000 rpm			±3	±2				
44	4	6	<1000 rpm	(S52) S6 (S33)	50	±50	±1.25	1	6	6	1
		(52)*	>1.5 sec			±5	±4				
		33	<450 psia			±20	±7				
54	5	6	<1000 rpm	(S52) S6 (S32)	50	±50	±1.25	1	6	6	1
		52	>1.5 sec			±5	±4				
		32	<450 psia			±20	±7				
71	7	6	<27,000 rpm	(S6 + S55) (S52)	100	±3	±3	1	4	4	1
		(52)*	>2 sec			±5	±4				
		57	>25 g's			±10	±5				

TABLE A-2 (Cont)

READI MODEL SYSTEM REQUIREMENTS

V	Malf. Area	Signal	Signal Processing	Definition of V (Boolean Notation)	Allowable Processing Time, msec	Allowable Error		Programmed Decision Number			
						V %	Processing Circuit %	Pre-Start	Start	Operate	Shutdown
83	8	3	<20 v	S3 (S6)	500	-	-50	2	1	1	2
		6	>0 rpm			+10	+8				
103	10	2	<20 v	S2 (S19)	100	-	-50	2	4	4	2
		19	Valve U4 closed			±2% of stroke	-				
111	11	3	<20 v	S3 (S16)	500	-	-50	2	1	1	2
		16	Valve U1 open			-	-				
122	12	23	<300 psia	S23 (S32) S24	4	±10	±5	1	4	4	1
		24	<100 psia			±10	±5				
		32	<750 psia			±10	±7				
132	13	23	>0 psia	S23 (S24)	4	±10	±5	10	10	1	10
		24	>10 psi			±10	±5				
141	14	33	<20 psia	S33 (S35) S37	1500	±10	±7	2	1	1	1
		35	<15 psia			±10	±7				
		(37)*	<30 sec			±10	±8				
151	15	(4)*	>20 v	S4 (S18)	1500	-50	-40	2	4	4	2
		18	Valve U3 open		4	±2% of stroke	-				
161	16	5	$S5 > 100^{e^{-\frac{(t-0.015)}{\tau}}} + 100$ $t = 0.050$; $t = 0.015$	S5		±10	-	1	7	7	1
						-	±7				
171	17	12	$S25 < 8.62\ (S12)^2\ S55 \times 10^{-5}$	S25	500	±1	±0.7	1	1	4	1
		25				±2	±1				
		55				±0.5	±0.3				

Table A-3

READI CORRECTIVE ACTION PATTERN FOR FAILURES IN ENGINE NUMBER ONE

Engine No.	Wire No.	Decision No.					
		1	2	4	6	7	10
1	1		1	1	1, 0	1, 0	1, [0]
	2					1, 0	1, [0]
	3						
2	1						
	2						
	3			1	1, [0]	1, [0]	
3	1						
	2						
	3			1	1, [0]	1, [0]	
4	1						
	2						
	3			1	1, [0]	1, [0]	
5	1						
	2						
	3			1	1, [0]	1, [0]	

Note:

1 = energize

0 = de-energize

, = 1 sec delay

[0] = conditional action

Appendix B

READI EQUIPMENT DESIGN CONSIDERATIONS

APPENDIX B

READI EQUIPMENT DESIGN CONSIDERATIONS

B-1. INTRODUCTION

A preliminary READI equipment specification broadly outlining the READI functional requirements was developed in Appendix A. However, the design of a READI system involves many trade-off considerations in addition to those reflected in this specification. Among the more important considerations discussed in this Appendix are:

- Reliability
- Transducer selection
- Stage vs. central vehicle computer
- Manned vs. unmanned vehicle application.

The trade-off evaluation of computer types is another vital equipment design consideration which is treated separately in Appendix C. This evaluation considers other merit factors such as cost, weight, versatility, and flexibility which influence computer circuit design.

B-2. RELIABILITY

Reliability and cost are the principal evaluation trade-off factors in evolving an optimum set of sensing parameters, malfunction indicators, and decision rules. These factors also influence the detailed design of the READI computer as developed in Appendix C. Analyses indicate, however, that for many READI functions the computer circuits can be designed to provide significantly greater reliability than the associated transducers. To simplify the relatively complex system evaluation, therefore, the contribution of electronic unreliability to total system unreliability can often be neglected.

To facilitate the evaluation of both the system and various computer types, three main reliability design criteria are established; namely, self-check, redundancy, and component reliability.

A. SELF-CHECK

There are two basic approaches to automatic, in-flight checkout of space vehicle electronic systems for improving operational reliability. The first consists of checkout equipment external to the system being tested. This approach is most advantageous where a number of vehicle systems are systematically checked from a central source. Diagnostic and confidence testing is often incorporated in such checkout systems to enabling the crew to aid in fault isolation and repair. The second approach is to provide built-in test equipment or internal self-check. This is the approach recommended for improving READI reliability, since it is relatively inexpensive and requires no external wiring.

The self-check design recommended for READI is completely automatic: the response time requirements of READI preclude any diagnosis, fault isolation, and corrective switching by the crew. In order to preserve the simplicity and reliability of the basic computer circuits, no repair capability is provided. Such repair capability with the associated redundancy requirements is often unnecessary. For example, self-check with no equipment redundancy can be used where awareness of system failure is sufficient to fulfill operational requirements as, for instance, in some man-machine systems. Self-check can also obviate or minimize redundancy requirements where continued equipment operation is of prime importance. Consider, for example, a redundant two-channel system with self-check of each channel. The ability to identify the particular channel failure by some simple internal detection means would eliminate the need for more complex triplicated channels. However, since self-check involves added equipment and complexity, if not unreliability of its own, the extent to which it is incorporated is determined by the best cost and reliability tradeoff.

Because transducers are the most costly and unreliable READI elements, failure detection of these components is the most significant self-check provision of any READI system. With self-check the requirements for either transducer or informational redundancy can be significantly reduced; this has been amply demonstrated in the READI evaluation. Transducer self-check can be accomplished with or without the use of input stimuli. The application of input stimuli for performing a complete transducer check is either impossible or impractical because of the complexity involved. For example, consider substituting differential pressure sensors for all pressure measurements in lieu of absolute pressure transducers.

A convenient, accurate pressure reference is provided to the low side of the sensors. This pressure is pulsed upon command of the self-check system and the response measured. Considering the complexity of the plumbing and degradation of sensor reliability, this technique has been discarded and more simple electrical measurement methods devised. Three reliable transducer check techniques appear to be most promising and have been incorporated in the model READI design.

The first is a measurement circuit designed to detect open and short circuits in the transducer output electrical elements and associated signal leads. Although this is an incomplete transducer test, it is significant in that the predominant failure of many sensors is electrical. The mechanical or prime mover unreliability not covered by this test can be statistically accounted for at another level of the system hierarchy.

The second transducer self-check technique consists of a comparator-detection circuit which functions to determine the reasonability of transducer output. The reasonableness check concept is based on the predictability of the maximum-minimum limits of transducer outputs. These limits are a function of either the maximum range through which the measured engine variable can traverse or the maximum operating range of the transducer. The detection of a signal above or below the known limits would indicate a failure in the transducer. A key advantage in this test method is that the entire transducer mechanism is checked. Such a check-out scheme, however, is not applicable to all the transducers selected for READI.

The third transducer self-check method is also based on the concept of transducer output reasonability. Instead of sensing level, the self-check circuit derives the rate-of-change of the measured engine parameters. This is compared to a stored value representing a maximum possible rate-of-change predicted for the variable for all conditions of engine operation. A transducer failure is indicated if this maximum limit is exceeded. As with the second self-check scheme, this test method cannot be applied to all the READI transducers.

Internal failure detection will also be required for computer circuits with unacceptably low reliabilities. One ground rule established in this case is that the circuits to be checked shall be considerably more complex and less reliable than the failure detection circuits. In the model READI system the principal circuits selected for check are the relatively complex, time-shared units (e. g. A/D converter, digital arithmetic computer). Such time-shared circuits

are most amenable to a programmed application of test stimuli and measurement of output response, and require a minimum of switching.

One self-check programming concept hypothesized is to test the READI transducers and certain computer elements only in response to a decision indication. The action associated with the particular decision output is delayed until the check-out is completed. When a decision is first sensed, a wired selection matrix will identify the transducers and computer circuits to be interrogated, i.e., all those components are tested which, under normal conditions, could have been instrumental in activating a known set of malfunction indicators and decision outputs. If the transducers and circuits tested are operating properly, the decision is then gated through. However, if it is determined that a transducer or circuit has failed, causing the decision, than the decision is inhibited and the failed element de-activated from the system. A central program can be used to control the sequence of operations during this check-out cycle.

This self-check procedure is intended to substantially improve reliability against false alarms, with or without redundant design. It is a relatively simple and reliable technique in that a minimum of control circuits are required. Where a transducer is checked by the reasonableness criteria, both the transducer and the test circuits must fail to produce the false alarm output. Thus, the net system false alarm unreliability is the product of the transducer and self-test unreliabilities, where the contribution of the computer electronics is assumed to be negligible.

One by-product of the false alarm self-check concept is to increase missed alarm unreliability. This results because of component deactivation from the system when it has been determined to have failed in a false alarm direction. Thus, the missed alarm failure rate of a component is adjusted to include the contribution of both missed and false alarm failure probabilities. However, the increased risk resulting from this higher missed alarm probability is considerably less than the reduction in risk effected by the improved false alarm reliability. This relationship is developed in Appendix A and it is shown graphically in figure A-1 where an incremental change in failure rate causes a much larger change in false alarm risk than missed alarm risk.

A logical extension of the self-test program would provide for an indication if a component has failed in a missed alarm mode. This implicitly suggests a somewhat more complex, continuous or

sequential interrogation of all transducers and circuits selected for test. Also implied in missed alarm failure testing is parallel redundancy with controlled switching between channels. An interlocking scheme can be arranged which would deactive the failed element and an alternate acceptable path would be traversed to the desired action. The value and potential uses of missed alarm self-check, and the associated redundancy required with such testing, must be evaluated for each malfunction detection branch. For that matter, the role of both false alarm and missed alarm self-check in the READI design can best be assessed in conjunction with the system evaluation of malfunction indicators and logical combinations of these indicators.

B. REDUNDANCY

Several redundant design techniques are available to improve reliability of performance. The impact of these design practices on reliability is basically that a single component failure will not cause a functional defect in the electronic package. Specific rules have been formulated for a computer evaluation of malfunction indicator redundancy based on cost-reliability trade-offs. There are basically two types of redundancy to be used in READI; informational and component. The nature of each is developed in Appendix K.

Of particular interest to the equipment designer, however, are the specific techniques of redundant operation. Consider a series array of elements A, B, C, D. To relate these elements to READI, assume A to be an engine, B to comprise a transducer and associated signal conditioner circuits, and C and D to represent computer blocks. Let us further suppose the reliabilities are analyzed and it is determined that B is a troublesome READI element. To alleviate the situation, the application of redundancy may be considered. It will be applied only to the B element since, to control cost and weight, it is advantageous to use as little redundancy as possible. Generally, there are two common accepted forms of redundancy, termed "parallel" and "parallel working". Parallel redundancy operates in conjunction with a two-position switch which is positioned to connect one of the two redundant B channels. Switching is an operation that must occur after a failure has been detected and isolated. Parallel working redundancy requires that the two identical B elements are present in the circuit continuously. Either element is capable of performing the B function in the event of a failure in the other element. This technique requires no failure detection circuits and is most commonly applied in analog circuits.

The signal space separation concept utilized in READI, however, presents an opportunity for a third redundant technique. Since many transducer signals are processed into 1, 0 Boolean states for deriving the malfunction indicators, the outputs of redundant transducer channels may be combined as AND or OR logical functions. Combining signals in this manner is much simpler than that associated with either parallel or parallel working redundancy. The digital logic redundancy technique is most useful in assigning reliability emphasis to either one of the two possible failure modes. For failure monitoring systems such as READI, these modes are termed missed alarm and false alarm. If we designate the binary state 1 to represent the indication of a malfunction, the use of the OR element will reduce the possibility of missed alarms, whereas the AND combination of binary signals would reduce the possibility of false alarms. There is no need for failure detection of either signal path to implement this redundancy technique. Equipment failure detection can be provided in conjunction with either logic approach to achieve a better balance in reliability improvement for both failure modes.

C. BASIC COMPONENT RELIABILITY

The failure rates assumed in statistically determining computer reliability are projected averages for microminiature components. Microminiature components are recommended for both analog and digital circuit design because of the significant reliability improvement anticipated within the next two to three years. There is a high degree of confidence throughout industry that integrated circuit failure rates of 0.05×10^{-6} per hour, or better, will be realized within this period because of the heavy investment (current and projected) in microelectronic development. This contrasts quite favorably with the average failure rates for ultra-reliable Minuteman ICBM components (e.g. 0.025×10^{-6} failures per hour for transistors). Minuteman components are extremely expensive, however, (20 to 30 times the cost of standard MIL approved components) and are still subject to failure probabilities in the wire interconnection.

The failure rates assumed in READI reliability analyses may or may not be achievable under the stresses of large liquid rocket engine environments, some of which are unknown. All component failure rate data is statistical in nature for some set of known conditions. Therefore, the effects of a severe booster environment on READI performance must be subjectively considered. Additionally, the extremely short mission times (approximately three

minutes for Saturn first stage) further introduces an unrealistic element in the reliability analyses. It has been demonstrated in solid-state electronics that turning a system on and off will introduce certain starting stresses. Some sources estimate that turning equipment on is equivalent to 35 to 60 hours of operation. These factors must be accounted for if valid reliability performance is to be realized. Accordingly, for the representative second stage READI, a time of two hours has been selected for computing failure probabilities. This is 40 times the actual mission time. It has also been assumed in the selection of failure rates that all components are aged until performance is along the random frequency portion of the failure frequency curve.

B-3. TRANSDUCER SELECTION CONSIDERATIONS

Without doubt the dominant requirement for transducers is high reliability. A concerted effort was made to uncover data on representative transducer failures in rocket engine environments. Rocket engine manufacturers have been cooperative in supplying data. However, care is necessary in interpreting transducer failure data because of such factors as:

- inclusion of failures other than the transducer; e.g. recording equipment
- some sensors were subjected to inputs or ambients beyond their design limits
- many failure reports include the remark "removed for failure or suspicion of failure", but follow-up data is not available from examination of the sensor
- many removals are for reasons of accuracy rather than failure.

Two conclusions drawn from the data analyses are: (1) pressure switches generally exhibit a high failure rate in rocket engine environments and should not be used with the READI system, and (2), if the transducer is relieved of the burden of incorporating its own reference level, it can be made more reliable.

A preliminary selection of sensor types has been made to meet the transducer requirements as interpreted from Appendix A, based mainly on achievement of good reliability. The two concessions

to high accuracy are the use of turbine meters for flow and the use of a few strain gauge pressure sensors. All transducers are within the current state-of-the-art.

Based on the available transducer failure data, analogy to rocket engine components of equivalent complexity, and some rough failure mode analyses, a list of high and low failure rates was generated. The failures are classified for "failed high" and "failed low" because the inadvertent action of READI will be directly influenced by sensor failures in the high and low direction. For instance, suppose that the normal condition of fuel pump output pressure during the operate phase is defined as greater than 900 psia. Then the failure of a pump output pressure sensor in the low direction would indicate a false alarm malfunction. Failure of the same sensor in the high direction might lead to a missed alarm if an engine failure did occur.

The need for high reliability, particularly low false alarm characteristics, has led to the incorporation of self-check provisions in the circuitry as described in the Reliability section of this Appendix. The self-check provisions look for shorts and opens in the electrical element of the sensor, check the outputs of reasonableness and eliminate some signals on the basis of excessive rates. The function of the self-test circuitry is to inhibit any action which would normally result from a failed sensor signal.

In the evaluation of the sample systems the nominal transducer failure rates were perturbed to 1/4 and 4 times the nominal. Another perturbation was also run where the failure rates were redistributed to account for the action of the self-check provisions of the equipment.

The accuracy with which a signal space separation must be made, as reflected in the allowable error in sensors and processing circuits, varies from ±50 percent to ±1 percent of full scale. The contribution to high and low failures of transducer inaccuracy varies from zero to as high as 15×10^{-4} in extreme cases where high accuracy is required. For the evaluation of trail systems the transducer failure rates were adjusted to account for the contribution of normal errors in the transducers and for failures in the processing circuits.

All of the sensors used in the sample system design are continuous analog devices, except the valve position sensors and the fire detector. The reference levels for sensors are stored in the electronics rather than in the sensors, for the following reasons:

- Sensor construction is simplified through the elimination of internal references
- A given sensor can be referenced or quantized to a number of different levels in different V's, and the proportional output can be used as well
- The reference can be changed during development more easily in the electronics than in individual sensors. (Several reference values must also be changed when the engine O/F or thrust is changed)
- The electrical part of the proportional sensors can be subjected to self-check.

Because of these considerations the use of pressure switches is not recommended in the READI system.

B-4. COMPUTER CONFIGURATION - INDIVIDUAL STAGE VS. CENTRAL VEHICLE COMPUTER

It was recognized early in the investigation that one question vitally affecting the system design had to be resolved. "What READI configuration best suits its application to a multi-stage launch vehicle?" It was essential that a practical scheme defining broad concepts of multi-stage READI design and integration be conceived before a detailed equipment design evaluation commenced. Two such schemes were selected for evaluation and a three-stage launch vehicle of an advanced Saturn type was assumed. One approach provides a separate, self-contained READI system for each propulsion stage. Each READI would be specifically designed, calibrated, and tested for its respective stage and operate virtually independently of the other stages comprising the vehicle. The second approach would provide a central computer shared among all three stages of operation. The computer was assumed to be installed in the standard instrumentation unit of the third stage. The semiconductor switching required to commutate engine transducer signals is installed in close proximity to the engines.

A comparative evaluation of both approaches was subsequently performed, the results of which are summarized for a number of merit factors.

A. OPERATIONAL RELIABILITY

The reliability of the separate stage computer approach is approximately 1.35 times better than that of the central computer

approach. This conclusion refers to each of both failure mode reliabilities which are defined as follows:

- The probability that a propulsion malfunction will be successfully detected over all three stages of operation
- The probability that a false alarm will not occur over all three sequenced stages of operation.

The superior reliability predicted for separate stage computers principally reflects the simpler design of an individual stage computer.

B. COST

Total cost of three separate stage computers is approximately 1.28 times the cost of the central computer system. Installation, as well as equipment costs, are included in this estimate.

C. EFFECTIVE WEIGHT

The effective weight of the central computer system is estimated to be 1.75 times the total effective weight of the three independent stage computers. Effective weight is a normalized quantity reflecting the added fuel penalties associated with increased weight in upper stages.

D. CABLING

The cabling problem presents a number of significant considerations. Some of the comments presented are qualitative in nature in that a more thorough examination of installation constraints and other cabling problems is required. However, certain cabling arrangements have been hypothesized for both system configurations for purposes of this evaluation. For the computer self-contained within a stage, parallel wiring has been assumed between all transducers and a single electronics package. The multiplexers are included in this package. For the central computer, well-shielded, high bandwidth transmission lines are assumed from each engine area to the instrumentation unit in the top of the vehicle. Within each stage the parallel wiring from the transducers is assumed to be connected to signal conditioner, multiplexer, and computer decommutation circuits located off the engines and in close proximity to the stage shell. Based on these assumptions it is concluded that

- Effective weight of cabling will be slightly less for the stage computer approach
- The long cables (over 300 feet for first stage data transmission) and umbilical interstage connections required for the central computer system are probably more susceptible to noise and resulting signal distortion. However, the magnitude of this problem is unknown
- The interstage connection of long cables required for the central computer introduces an element of additional unreliability
- Cable installation costs will undoubtedly be higher for the central computer
- Wiring among the central READI computer and displays, pilot controls, and guidance and control computer is considerably less than that required for separate stage computers
- Wiring between individual stage computers and launch vehicle systems contained within each stage is considerably less than that required for a central computer system. These systems include telemetry, ground support, equipment propellant utilization, and thrust vector controls.

E. INTERSTAGE DATA FLOW REQUIREMENTS

Although a READI system functions to monitor the propulsion system for possible malfunction only during operation of a stage, it is conceivable that information on previous stage performance would be useful in establishing optimum decisions for subsequent powered flight. Only data representing a gross measure of propulsion performance is required, such as that provided by the malfunction indications and associated actions generated by READI. Time of malfunction occurrence would also be required. Such a requirement for inter-stage data transmission necessitates a functional compatibility between the various stages of READI operation. To achieve this compatibility, additional cabling, interconnections, and integrated design effort is required for the stage computer approach over that required for the central computer approach.

F. CAPABILITY FOR FUNCTIONAL EXTENSION (GROWTH POTENTIAL)

Appendix B outlines some of the interface considerations between READI and various vehicle subsystems. One of the major considerations involves the potential contribution a READI system can make in simplifying a system such as ground support equipment (GSE). Since GSE is designed to check out each individual stage independently of the launch vehicle, a complete READI system self-contained within each stage is required if any GSE-READI integration is to be achieved.

G. ADAPTABILITY TO VARIOUS MISSION-VEHICLE COMBINATIONS (FUNCTIONAL FLEXIBILITY)

The large number of engines and stages which are planned or under development will ultimately provide NASA with a versatile inventory of propulsion systems capable of being used in a variety of launch vehicle configurations serving different missions. This fact is perhaps the most important criteria dictating a separate stage design approach for READI because:

- The most efficient means of evolving a READI system to operational status for a given vehicle is to phase the READI design into the stage contractors development and test programs. This infers that separate prototype READI systems be provided for each stage selected for READI utilization. Although a central computer system is shared among stages during operation, a separate prototype would be required to test each stage for which it was designed, resulting in a more costly prototype development.
- Since the central computer contemplated is of a special purpose type, the extent to which its program can be altered is limited without extensive redesign. This would present a problem if a requirement existed to modify the computer for use in vehicles containing engines other than those for which the computer was designed. Only with a larger, more complex general purpose machine could such flexibility be effectively achieved. A stage computer on the other hand is designed virtually independent of the launch vehicle. It is readily adaptable to other stages containing a different number of the

same engines. These considerations, coupled with the knowledge that many stages already contracted are slated for more than one vehicle block, suggest that READI development be directed to specific stage designs.

- The task in programming a READI for different missions is about the same for both system approaches.
- The time required to develop a central READI computer system for a three-stage vehicle will undoubtedly be longer than that required for separate stage designs.

Based on results of the evaluation, it is recommended that:

- The design and mechanization of a READI system for a multistage vehicle be effectively divided between the individual stages, with a separate computer provided for each stage.
- The design of each stage oriented READI system be coordinated such that a functionally integrated vehicle READI system is realized. Compatible design between stages reflecting signal sensitivity, impedance matching, interconnection, and other considerations should be emphasized in the READI development.
- The mission contractors coordinate with the READI contractor the requirements for inter-stage data integration between READI and other launch vehicle subsystems; the mission contractors supply to the READI contractor the mission data and criteria which affect the computer programming of decisions. This coordination should be phased early in the READI development program.

B-5. MANNED VS. UNMANNED VEHICLE APPLICATION

Minimum crew safety and mission accomplishment reliabilities are key criteria specified by the mission contractor and used in the system evaluation and optimization. In addition, these parameters significantly affect the computer mechanization concept to be selected. The economics of an operational READI clearly dictates the requirement for flexibility in reliability design. More specifically, any READI designed for a specific stage should be capable of

- providing reliability performance so weighted between missed alarm and false alarm modes as to satisfy acceptable reductions in mission accomplishment and crew satety risks for any weighting of these factors. This also applies to the special case of unmanned flight
- being readily adaptable with minimum equipment modification to a change in reliability requirements for both failure modes as dictated by the crew safety and mission accomplishment weighting.

A high priority has been established for this design goal. This is reflected in the flexibility merit factor used in the "Trade-off Evaluation of Computer Types" presented in Appendix C.

Appendix C

TRADE-OFF EVALUATION OF COMPUTER TYPES APPLICABLE TO READI

APPENDIX C.

TRADE-OFF EVALUATION OF COMPUTER TYPES APPLICABLE TO READI

C-1. GENERAL

The operational requirements in Appendix A and the equipment design considerations in Appendix B define the functional requirements of a READI system. Four candidate systems, based upon the requirements in Appendices A and B, have been competitively evaluated. They are:

- Continuous Analog System
- Analog Sampled Data System
- Serial Digital Computer
- Hybrid of the Continuous Parallel Analog System and Serial Digital Computer.

To simplify the evaluation of the competitive systems, the functions defined in Appendix A will be separated into two general categories according to their relative equation complexity.

- Simple functions - signal space separations containing elementary equations
- Complex functions - signal space separations containing involved equations.

The candidate systems utilize circuits and components for certain functions which are similar in their cost, complexity, and reliability. This similarity allows them to be eliminated in the evaluation of the candidate systems. The components and circuits considered equivalent in this evaluation are:

- Transducers
- Transducer self-check
- Decision logic
- Output circuits.

A detailed description of the operational and circuit requirements of these functions appears in Appendices B and E.

C-2. EVALUATION CRITERIA

There are three prime factors in determining the merit of each of the candidate systems. They are, in order of importance: reliability, flexibility, and versatility, and cost. A discussion of each of these criterion follows:

A. RELIABILITY

Two modes of failure are considered in the design of a reliable READI system.

1. False Alarm

Failure of a component in READI in such a direction as to indicate a malfunction in the engine when no malfunction exists is called a false alarm. For this evaluation, the malfunction detection channel false alarm rates of the candidate systems are compared to the desired false alarm rate for a typical channel. The curve in figure A-1 represents the sensitivity of mission risk to READI failure rate for a typical channel. The most desirable false alarm rate is, of course, the one which yields the least risk. However, in the design of a specific channel, if redundancy and/or self-check is contemplated, a point of diminishing returns is reached where the cost of implementing this additional circuitry is greater than the return due to the reduction of mission risk. By the use of this sensitivity curve, the optimum false alarm rate (λ_f) is selected and evaluated for each of the candidate systems.

2. Missed Alarm

Failure of a component in READI, causing a failure to indicate a malfunction in the engine when a malfunction has occurred, is a missed alarm. For this evaluation, the missed alarm rates (λ_m) of the candidate systems are compared to the desired missed alarm rate of a typical channel. The sensitivity of mission risk to the equipment failure rate is illustrated in figure A-1. The reduction in missed alarms by the use of redundancy techniques is desirable only if the value of the resulting reduction in mission risk is greater than the costs incurred by addition of these redundant circuits. Comparison of these costs and missed alarm rates of the candidate systems is used to determine the optimum system.

B. FLEXIBILITY AND VERSATILITY

The design of the optimum system must be such that it is capable of adapting to varying requirements and additional tasks. The ability of READI to be modified and expanded, and to reliably perform its function with various combinations of missions and vehicles is a vital factor in the selection of the optimum system.

C. COST

Each candidate system incurs certain costs due to the circuits required for engine data processing. The other criteria for the optimum system may be attainable, but in some candidate systems the cost of meeting these requirements is high. These high costs reduce the value of READI; therefore, the circuit costs of the candidate systems are compared as to their effect on the mission value of the competing systems.

By the use of figure A-1, the false alarm rate (λ_f) and missed alarm rate (λ_m) of a channel in a candidate system are converted to two associated losses in the value of READI:

ΔV_f - loss in READI value due to false alarms

ΔV_m - loss in READI value due to missed alarms.

Therefore, the total loss in the value of READI, L, may be evaluated by summing up the cost of the circuits, the loss in READI value due to false alarms (ΔV_f), and the loss in READI value due to missed alarms (ΔV_m) or

$$L = \text{circuit cost} + \Delta V_f + \Delta V_m$$

In the evaluation of the candidate systems the reliability and circuit costs will be summed into one figure: the total loss in the value of READI, L. This figure and the relative flexibility and versatility of the competing systems will form the basis for the selection of the optimum READI implementation.

In addition to the three prime factors emphasized, there are other criteria which should be considered in evaluating the candidate systems. Although these factors are of secondary importance, they will influence the selection of the optimum READI system:

- Effective weight
- Processing speed
- Volume
- Power
- Integration with other Launch Vehicle Systems
- Development risks
- Installation.

C-3. DESCRIPTION AND EVALUATION OF CANDIDATE SYSTEMS

A. CONTINUOUS ANALOG SYSTEM

The continuous parallel analog system, figure C-1, provides independent malfunction detection channels for READI functions. A complete and separate system is used with each engine; no multiplexing is employed.

The majority of malfunction detection channels is simple functions requiring signal conditioning and Boolean logic circuits which are simple and reliable. Figure C-2 is a block diagram illustrating the implementation of a simple function. The calculated false alarm probability, missed alarm probability, and cost for this circuit are

$$\lambda_f = 0.05 \times 10^{-4}$$

$$\lambda_m = 0.2 \times 10^{-4}$$

$$\text{Cost} = \$175$$

Redundancy techniques may be applied to these simple circuits to obtain a higher channel reliability. However, the maximum gain in value for a reduced false alarm rate (ΔV_f) or for a reduced missed alarm rate (ΔV_m) determined from the curve of a typical channel, figure A-1, is

$$\Delta V_f = 160$$

$$\Delta V_m = 0$$

The use of redundancy techniques to reduce the false alarm rate, therefore, does not add to the value of READI, due to the cost of the added circuits.

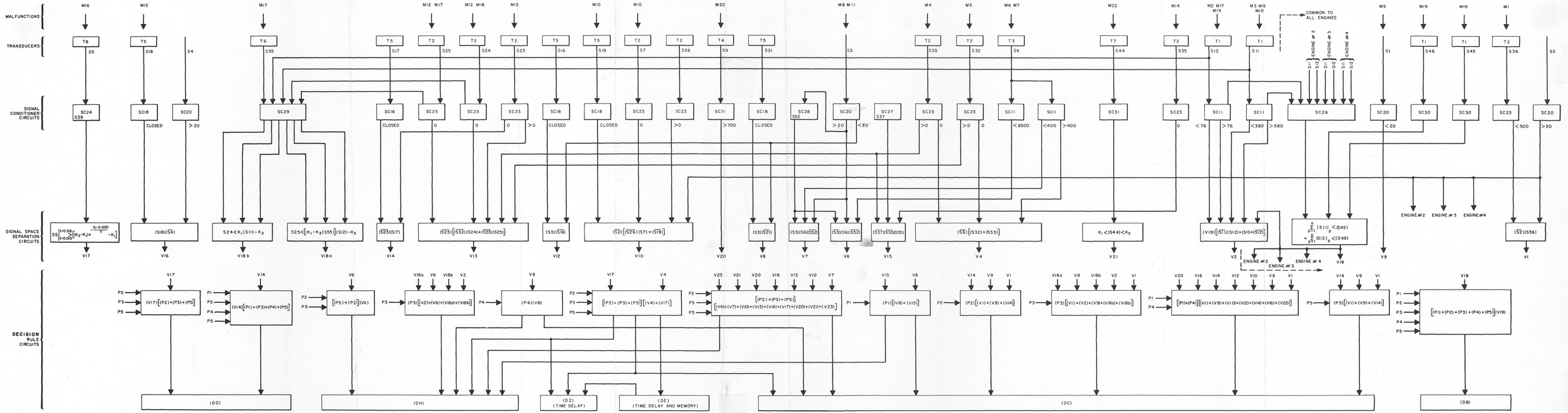


FIGURE C-1
CONTINUOUS ANALOG SYSTEM

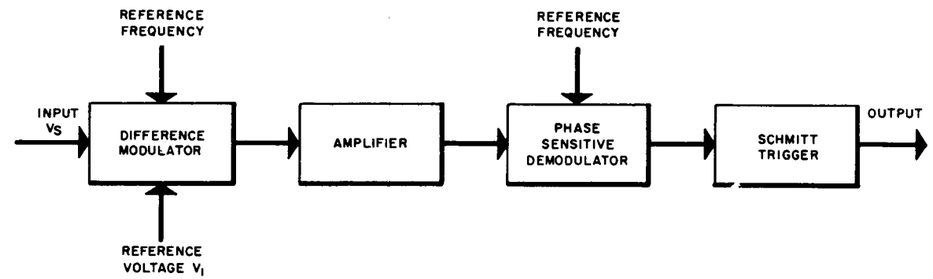
TYPICAL SIGNAL CONDITIONER - SC 20

FUNCTION:	Voltage level detector
INPUT:	DC Amplitude V_s
OUTPUT:	"O" For $V_s < V_l$ "1" For $V_s > V_l$
SENSITIVITY:	Change in state when $V_s \geq V_l$
RELIABILITY:	$\lambda_f = 0.05 \times 10^{-4}$ $\lambda_m = 0.2 \times 10^{-4}$
ACCURACY:	±5% of V_l
SIZE:	2.96 $in.^3$
WEIGHT:	0.24 lb
POWER:	120 mw

READI FORM NO. 2

TYPICAL SIGNAL CONDITIONER - SC 20

CIRCUIT:



READI FORM NO. 2

FIGURE C-2
TYPICAL SIGNAL CONDITIONER - SC 20
SIMPLE FUNCTION

These simple functions require such elementary circuits that only slight modifications on a few basic configurations provide circuits which are applicable to many types of transducers. The continuous parallel-wired system, therefore, is reliable, versatile, and flexible when simple functions are implemented.

The remaining channels, however, perform complex functions which require involved circuitry to attain the accuracies specified. The application of self-check and/or redundancy techniques to these circuits to obtain the false alarm and missed alarm probabilities desired increases the hardware complexity substantially. A typical complex function, figure C-3, may be implemented with the following characteristics:

$$(\lambda_f) = 0.36 \times 10^{-4}$$

$$(\lambda_m) = 1.09 \times 10^{-4}$$

$$\text{Cost} = \$500$$

Referring again to figure A-1, the maximum gains in the value of READI due to a decrease in the false alarm and missed alarm rates are

$$\Delta V_f = \$1200$$

$$\Delta V_m = \$15$$

To decrease the false alarm rate of this circuit, a redundant circuit identical to the one illustrated in figure C-3 is AND gated with the original circuit. The following characteristics result:

$$\lambda_f = 0.013 \times 10^{-4}$$

$$\lambda_m = 2.2 \times 10^{-4}$$

$$\text{Cost} = \$1100$$

$$\Delta V_f = \$40$$

$$\Delta V_m = \$30$$

The equation for the loss in value to READI is

$$L = \text{circuit cost} + \Delta V_f + \Delta V_m$$

The calculated losses for the two circuits are

no redundancy

$$L = \$1715$$

with redundancy

$$L = \$1170$$

The circuit implementing redundancy results in a gain in the value of READI of $545. The use of further redundancy, however, would not be of any value to READI due to the high cost of the circuits required.

The circuits implemented for the complex functions are designed specifically to perform the limited operations required for the particular malfunction detection channel. Should the requirements vary sufficiently because of a change in the mission or vehicle, the circuit would require extensive redesign. A mission or vehicle change would also result in the creation of new functions to be implemented, requiring the complete replacement of channels or the addition of complex circuits to perform the functions. Development and test of all possible malfunction detection channels would be required to insure that READI reliably performs its operational requirements. This system approach, therefore, has a distinct limitation in its versatility and flexibility.

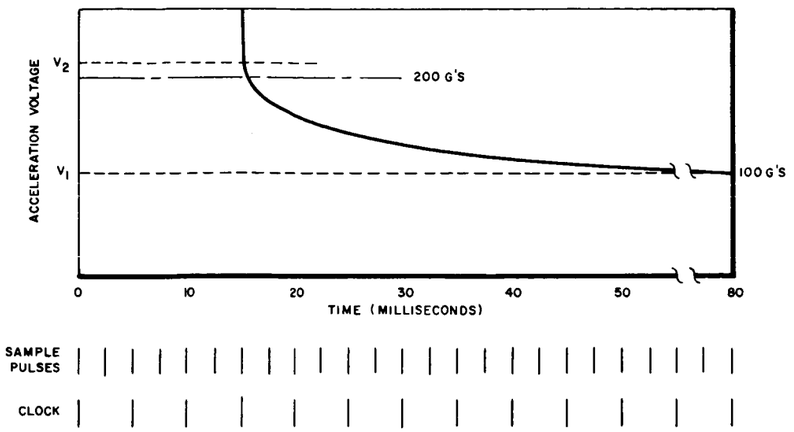
B. ANALOG SAMPLED DATA SYSTEM

The analog sampled data system, figure C-4, is a central-programmed computer which time-shares an analog comparator and analog computer circuits. The majority of the engine transducer outputs is multiplexed through the analog comparator whose output is decommutated and stored. The balance of the engine transducer outputs is multiplexed through the computer circuits and is also decommutated and stored. These stored outputs are then operated on by simple Boolean logic circuits for processing by the decision logic circuits.

The simple and complex functions are processed by circuits which are identical to those described in the previous system. By multiplexing the signals into common circuits, the cost incurred by each malfunction detection channel is now reduced. The simple functions, however, cost approximately the same because the multiplexing switches and control circuitry required are comparable to the malfunction detection channel costs of the previous system.

TYPICAL SIGNAL SPACE SEPARATION - SC 24

FUNCTION: Amplitude vs. Time Limit Comparator



INPUT: AC Amplitude

OUTPUT: "1" for $V(t) > (V_2 - V_1)\, e^{-\frac{(t - 0.015)}{RC}} + V_1$ $\quad t = 0.015 \text{ to } t = 0.08$

"O" for $V(t) < (V_2 - V_1)\, e^{-\frac{(t - 0.015)}{RC}} + V_1$ $\quad t = 0.015 \text{ to } t = 0.08$

(t = seconds)

SENSITIVITY: Change in State When

$V(t) > (V_2 - V_1)\, e^{-\frac{(t - 0.015)}{RC}} + V_1$ $\quad t = 0.015 \text{ to } t = 0.08$

RELIABILITY: $\lambda_f = 0.36 \times 10^{-4}$

$\lambda_m = 1.09 \times 10^{-4}$

ACCURACY: ±10%

SIZE: 6.29 $in.^3$

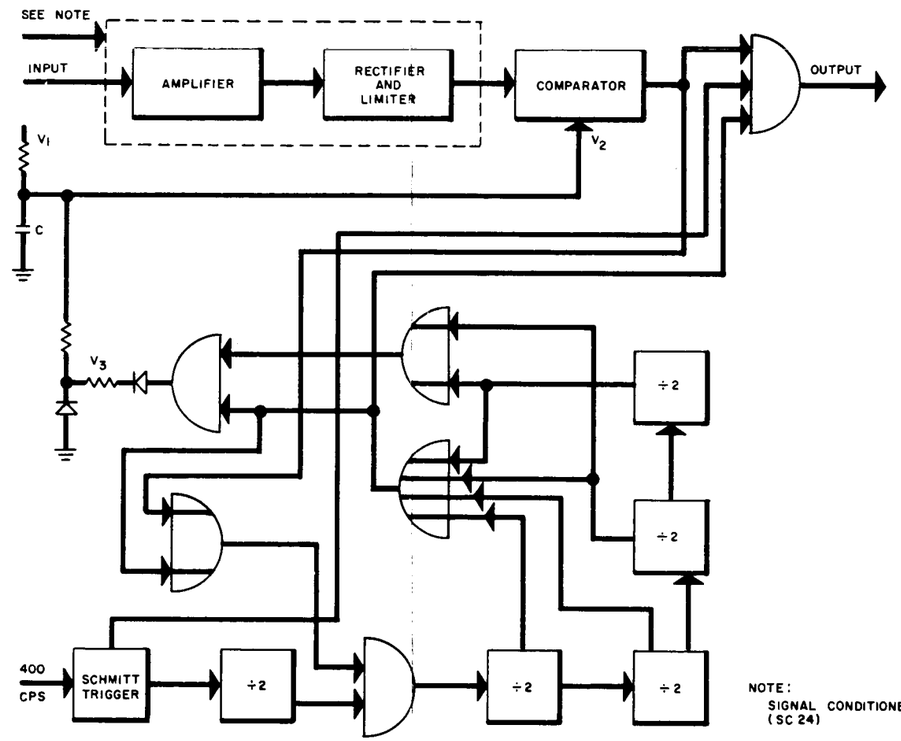
WEIGHT: 0.049 lb

POWER: 260 mw

READI FORM NO. 2 Sheet 1 of 2

TYPICAL SIGNAL SPACE SEPARATION - SC 24

CIRCUIT:



READI FORM NO. 2 Sheet 2 of 2

FIGURE C-3
TYPICAL SIGNAL CONDITIONER - SC 24
COMPLEX FUNCTION

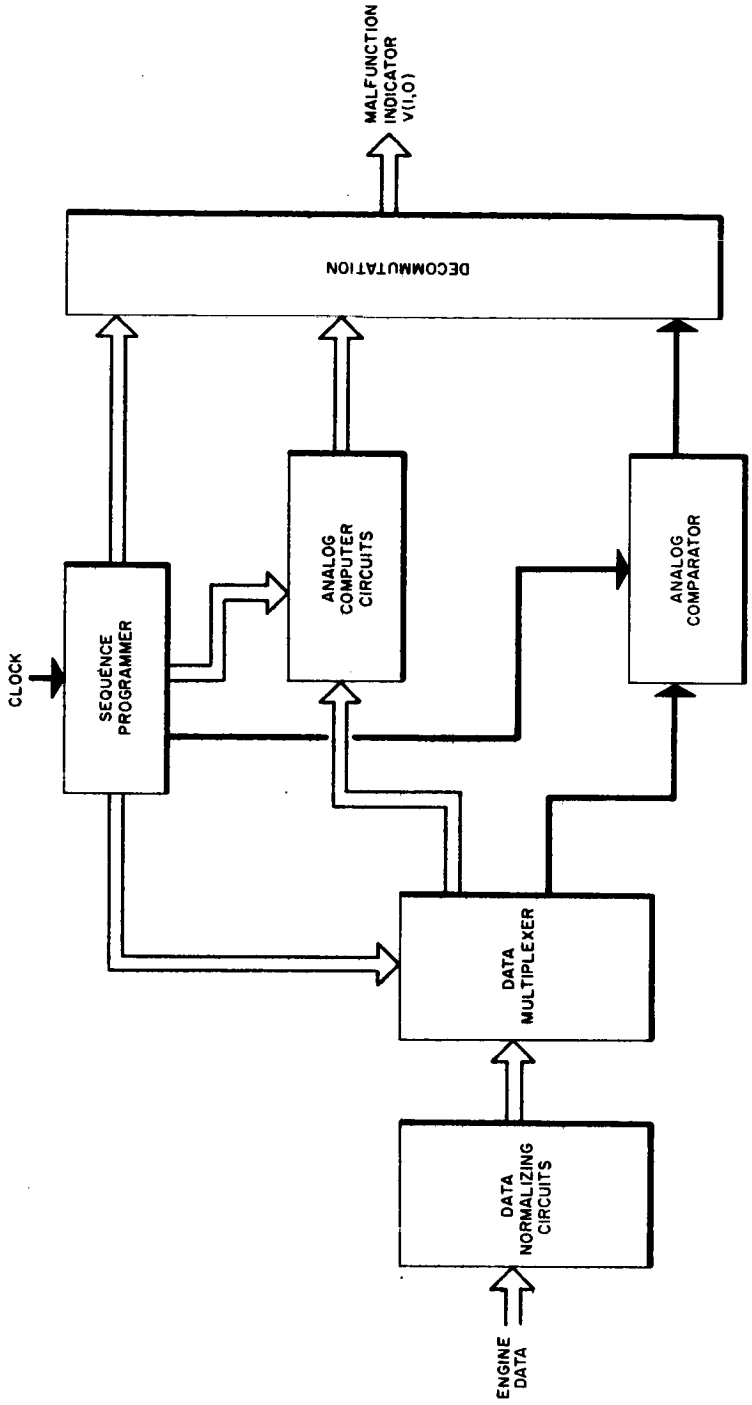


FIGURE C-4

ANALOG SAMPLED DATA SYSTEM

The characteristics of the circuits required for the simple and complex functions, including the unreliability of the multiplexing switch, (0.05×10^{-4} for both missed alarm and false alarm) are shown in table C-1. Both the simple and complex functions increase in value when redundancy is implemented to reduce the false alarm rate. However, further use of redundancy on these circuits will not yield an increase in the value of READI because the loss of value, L, is due mostly to the circuit costs and not to the failure rates.

The implementation of analog computer circuits for the complex functions still results in a system which has poor flexibility as explained in the continuous analog system. Although engines may time-share the computer circuits, the ability of the circuit to be adapted to meet new requirements is still very limited. The development and test of a selection of these special circuits is still required.

TABLE C-1

ANALOG SAMPLED DATA SYSTEM

	λ_f x.10+4	λ_m x 10+4	Cost ($)	ΔV_f ($)	ΔV_m ($)	L ($)
Simple Function						
Without redundancy	0.1	0.25	175	300	0	475
With redundancy	0.013	0.5	300	0	80	380
Complex						
Without redundancy	0.41	1.14	225	1400	17	1642
With redundancy	0.013	2.3	500	0	37	537

λ_f = false alarm rate

λ_m = missed alarm rate

Cost = circuit cost

ΔV_f = loss in READI value due to false alarms (figure A-1)

ΔV_m = loss in READI value due to missed alarms (figure A-1)

L = total loss in the value of READI

where $L = \text{cost} + \Delta V_f + \Delta V_m$

C. SERIAL DIGITAL COMPUTER

The serial digital computer system, figure C-5, performs all READI functions, sequentially time-sharing an analog-to-digital converter and digital computer. All the engine transducer inputs are multiplexed and converted to binary form for computer processing. All comparator functions, algebraic functions, and Boolean logic functions are performed digitally in serial form by the computer programmed by a fixed-wired memory.

The multiplexing of all signals through a single analog-to-digital converter and digital computer provides a simple and reliable means of employing computer self-check. If known input stimuli are encoded by the analog-to-digital converter and processed in accordance with the special program provided in the computer, the system may be checked for proper operation. The binary words of the encoder and memory are also checked for singular bit errors by the use of parity check. Detection of a bit error or improper computer operation nullifies any potential decision which the system may have stored for implementation.

Self-check of the computer is considered essential because of the relatively poor false alarm rate (2×10^{-4}). The following channel characteristics are applicable to the simple and complex functions because the computer is time-shared by both:

$$\lambda_f = 0.05 \times 10^{-4}$$

$$\lambda_m = 4 \times 10^{-4}$$

$$\text{Cost} = \$500$$

$$\Delta V_f = \$160$$

$$\Delta V_m = \$70$$

$$L = \$730$$

A further decrease in the loss of READI value may be acquired by using redundant multiplexing switches which will reduce the false alarm rate. However, the main loss of value in the system is the increased cost of the circuits required for the simple functions. Simplification of the computer would be required to attain this cost decrease, and this is impossible due to the number of signals to be processed.

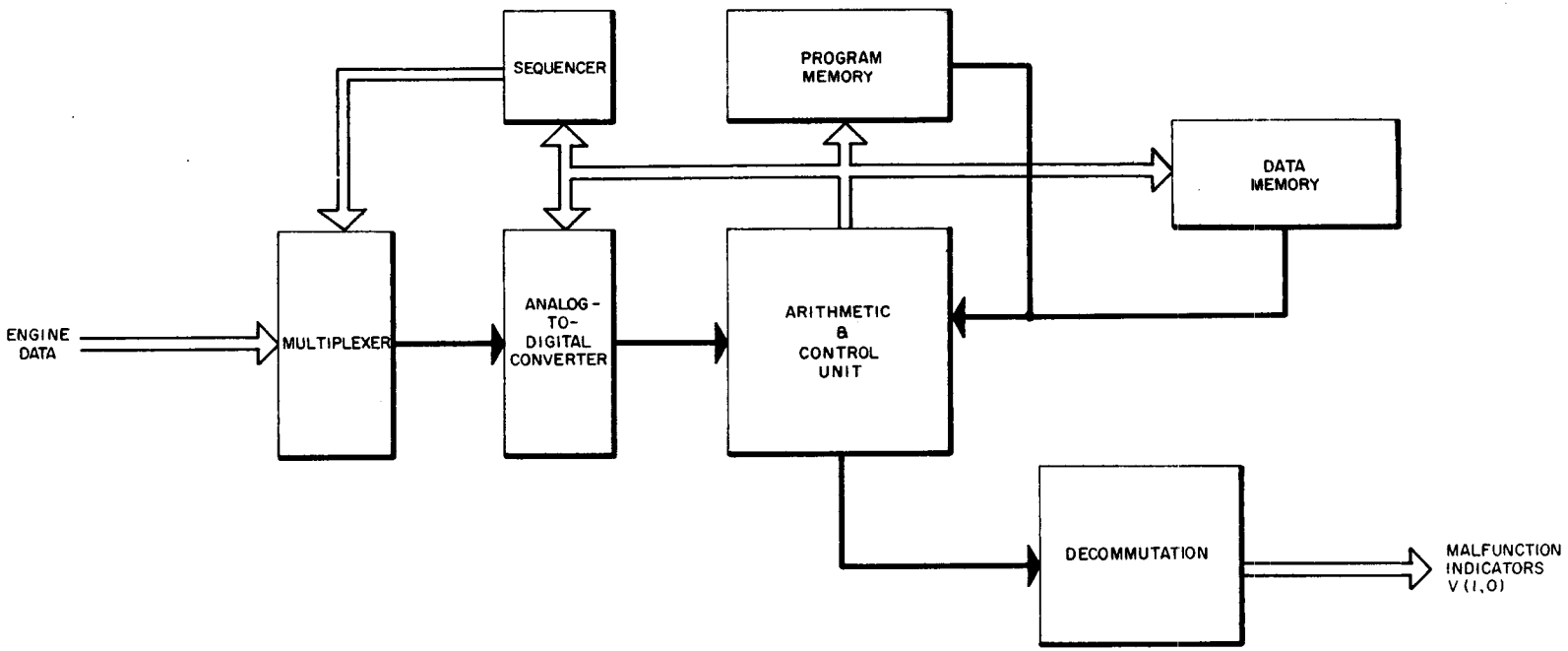


FIGURE C-5
SERIAL DIGITAL COMPUTER

A factor which becomes significant in this system, which did not require investigation in the previous systems, is the required speeds for signal processing. Table A-2 in Appendix A lists the processing times of the various signal space separations. Using a serial digital computer to process these signals at the required rates operates the computer in a region close to its maximum data handling capability. Should the mission or vehicle change sufficiently to increase the complexity or the number of signals requiring fast processing times, the computer would require redesign to improve its speed.

The serial digital computer is a very versatile and flexible machine within its operating capabilities. By relatively simple changes in the program and data memories, complex functions may be altered or added.

D. HYBRID SYSTEM

In the evaluation of the three previous systems, it became apparent that some combination of these systems might be selected which would retain the advantages of a particular system, while not incurring the disadvantages of the system.

The hybrid system selected, figure C-6, utilizes the continuous, malfunction detection channels for the simple functions and a serial digital computer for the complex functions. The characteristics of the hybrid system are shown in table C-2. The use of the parallel-wired channels removes some of the burden from the serial digital computer, thus providing the system with additional capacity to accept complex functions requiring fast processing times.

TABLE C-2

HYBRID SYSTEM (SINGLE CHANNEL)

	λ_f x 10^{+4}	λ_m x 10^{+4}	Cost ($)	ΔV_f ($)	ΔV_m ($)	L ($)
Simple Functions	0.. 05	0. 2	175	160	0	335
Complex Functions	0.. 05	4	700	160	70	930

λ_f = false alarm rate

λ_m = missed alarm rate

Cost = circuit cost

ΔV_f = loss in READI value due to false alarms (figure A-1)

ΔV_m = loss in READI value due to missed alarms (figure A-1)

L = total loss in the value of READI

The continuous malfunction detection channels and the serial digital computer are both amenable to alterations, if required by a mission or vehicle change. The parallel-wired system, because of its simplicity, may be altered readily, and the digital computer may be changed easily by altering its wired memory. The system is, therefore, quite flexible and versatile.

C-4. CONCLUSIONS

To aid in the evaluation of the candidate system, two tables were developed: one for the simple functions, and one for the complex functions. The figures presented in each of the tables are based upon the circuits which yielded the optimum value to READI. Therefore, the figures may, in some instances, be those obtained by the use of redundancy.

The evaluation data for the simple functions appear in table C-3. The reliabilities of all the candidate systems (λ_f and λ_m) are good, and therefore, the loss in the value of READI due to missed alarm (ΔV_m) and false alarm (ΔV_f) is low. The systems with the lowest circuit costs are the continuous analog system and hybrid system, with the other two candidates showing a marked increase in this area. In evaluating the value to READI of each candidate system, the continuous parallel system and hybrid system have a slight edge. In the evaluation of the versatility and flexibility of the candidate systems, the serial computer is superior. However, this rating must be qualified because the amount of data being handled is assumed to be well within the capacity of the machine, which may not be the case if the system is required to accept many new high data rate signals. The candidate systems selected for processing simple functions, based upon this evaluation, are the continuous analog system and the hybrid system.

The evaluation data for complex functions are tabulated in table C-4. Here again, the reliability data for the candidate systems (λ_f and λ_m) are good, resulting in relatively low losses in the value of READI due to missed alarms (ΔV_m) and false alarms (ΔV_f). The analog sampled data system and serial digital computer both have the same circuit costs with the hybrid system next, followed by the continuous analog system. The candidate system which yields the greatest value of READI is the analog sample data system; however, this system is not very flexible or versatile. The serial digital computer is next in READI value and has excellent versatility and

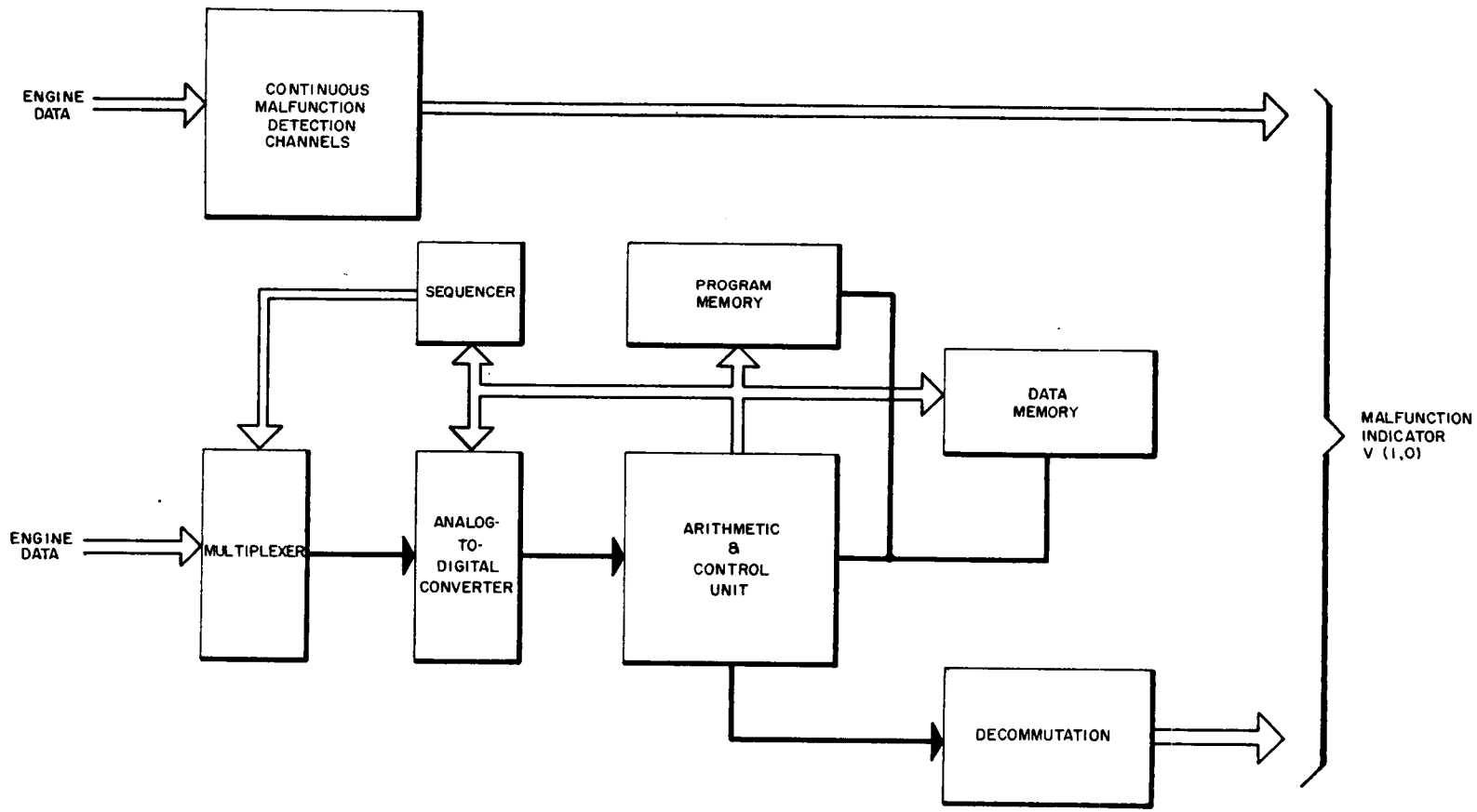


FIGURE C-6
HYBRID SYSTEM

flexibility; however, this last factor must be qualified because of the upper limit on its data handling capacity. The hybrid system yields the next higher value of READI and has excellent versatility and flexibility. Based upon the possible amount of data to be handled and this evaluation, the hybrid system was selected to process the complex functions.

The hybrid system, selected as the optimum system for both simple and complex functions, is proposed as the system to be implemented for READI.

TABLE C-3

CANDIDATE SYSTEMS EVALUATION DATA (SINGLE CHANNEL)
SIMPLE FUNCTIONS

Candidate Systems	λ_f x 10^{+4}	λ_m x 10^{+4}	Cost ($)	ΔV_f ($)	ΔV_m ($)	L ($)	Versatility and Flexibility
Continuous Analog System	0.05	0.2	175	160	0	335	Good
Analog Sampled Data System*	0.013	0.5	300	0	80	380	Fair
Serial Digital Computer	0.05	4	500	160	70	730	Excellent
Hybrid System	0.05	0.2	175	160	0	335	Good

*redundancy used

λ_f = false alarm rate

λ_m = missed alarm rate

Cost = circuit cost

ΔV_f = loss in READI value due to false alarms (figure A-1)

ΔV_m = loss in READI value due to missed alarms (figure A-1)

L = total loss in the value of READI

TABLE C-4

CANDIDATE SYSTEMS EVALUATION DATA (SINGLE CHANNEL)
COMPLEX FUNCTIONS

Candidate Systems	λ_f x 10^{+4}	λ_m x 10^{+4}	Cost ($)	ΔV_f ($)	ΔV_m ($)	L ($)	Versatility and Flexibility
Continuous Analog System*	0.013	2.2	1100	40	30	1170	Poor
Analog Sampled Data System*	0.013	2.3	500	0	37	537	Poor
Serial Digital Computer	0.05	4	500	160	70	730	Excellent
Hybrid System	0.05	4	700	160	70	930	Excellent

*redundancy used

λ_f = false alarm rate

λ_m = missed alarm rate

Cost = circuit costs

ΔV_f = loss in READI value due to false alarms (figure A-1)

ΔV_m = loss in READI value due to missed alarms (figure A-1)

L = total loss in the value of READI

Appendix D

INTEGRATION OF READI WITH THREE STAGE LAUNCH VEHICLE

APPENDIX D

INTEGRATION OF READI WITH THREE-STAGE LAUNCH VEHICLE

D-1. THREE-STAGE READI CONFIGURATION

The individual READI stage development concept was developed in Appendix B. This appendix describes the READI configuration for a typical multi-stage vehicle and the functional-physical interface of each READI to the various subsystems of the vehicle. Additionally, recommendations are presented on the installation and electrical interconnection of READI within the vehicle.

The launch vehicle assumed is comprised of three stages with a manned spacecraft payload. The READI function is applied in this example only to the three main booster stages; no monitoring has been included for any space engines which may be contained in the spacecraft. The upper stage is assumed to have space maneuvering capability. It consists of one engine identical to the model READI engine hypothesized for the second stage. The second stage is comprised of five model READI engines. The first stage also includes five engines, typically of the LOX-RP1 type, with no restart capability.

Figure D-1 illustrates the functional integration of READI to such a three-stage launch vehicle. The interface between each READI stage to the various vehicle subsystems is outlined in succeeding sections of this appendix. Only the second-stage interface is shown in detail since the interface within the other stages is quite similar. In addition, the installation concepts described later in this appendix apply to all three-stage READI systems.

The physical characteristics of each stage READI are estimated to be as shown in table D-1.

D-2. SYSTEMS INTERFACE

A. INTRODUCTION

An important consideration in the development of READI for an operational vehicle is the interface with other launch vehicle systems and ground-based control and support systems. Detailed

TABLE D-1

READI PHYSICAL CHARACTERISTICS

	STAGE 1		STAGE 2		STAGE 3	
	Transducers	Computer	Trans.	Comp.	Trans.	Comp.
Weight* (lb)	90	30	140	35	25	15
Volume (cu in.)	-	410	-	530	-	190
Power (watts)	-	42	-	55	-	18

*Includes weight of pressurized inert gas containers and cabling between READI equipment.

studies must be carried out in this area by the READI, stage, and mission contractors to ensure that a READI system is compatible with mission operational procedures and all input-output data transmission requirements. Therefore, a preliminary READI interface study was conducted for an advanced Saturn type vehicle. The principal objectives were to:

- Define the inter-relation and command priority assignments between READI and other systems, manual and automatic, as they may affect and possibly constrain the decision making authority of READI.
- Define the input-output informational requirements.
- Examine areas of potential trade-off in equipment consolidation and functional integration considering signal form and accessibility.

B. GROUND SUPPORT EQUIPMENT – READI INTERFACE

An automatic checkout system is projected for advanced, multi-stage vehicles which will provide a systematic and thorough evaluation of the propulsion systems. Ground support equipment (GSE) peculiar to each stage forms part of this system and functions to distribute vehicle system data to a central control facility. This facility contains launch support equipment common to all vehicles and functions to remotely control and evaluate an elaborate and detailed sequence of tests on the vehicle. Digital data-handling machines are included in this facility.

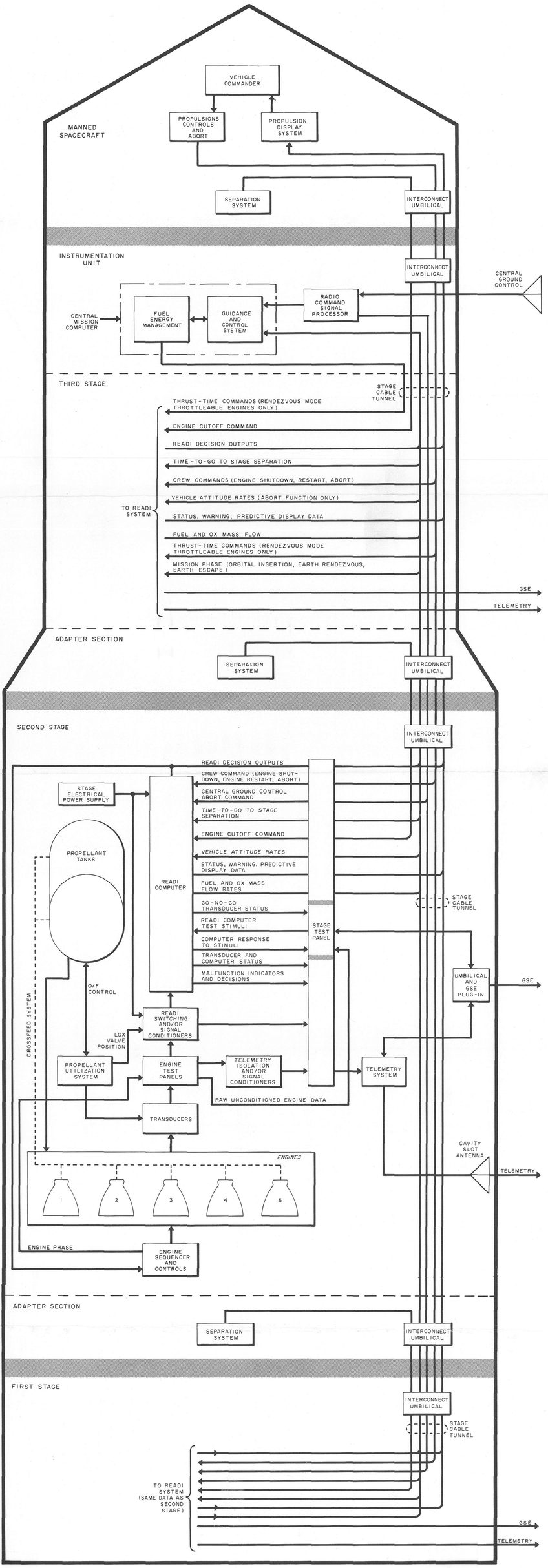


FIGURE D-1
READI SYSTEMS INTERFACE
FOR THREE STAGE LAUNCH VEHICLE

The Saturn automatic checkout scheme, for example, begins with individual stage testing at the contractor's plant followed by test firing at the Marshall Space Flight Center. The GSE test operations at the AMR launch site begin with individual checkout and readiness tests of each stage. Following completion of these tests, the stages are assembled and retested concurrent with a series of other vehicle system tests. The remaining test operations involve final checkout and countdown for launch.

The GSE system for advanced vehicles will undoubtedly mechanize a very sophisticated testing concept. The data processed by GSE will permit a thorough assessment of the booster status with the aid of the digital computer in central control. Some of the GSE-READI data integration requirements conceived are:

- Propellant and engine status information will be supplied to GSE by READI. This will include both raw, unconditioned transducer signals and processed data. The latter would generally be in qualitative form and is intended to simplify both the GSE equipment and calibration procedures. When the engines are inoperative, certain signals such as rpm, fuel flow, etc., are not provided.
- GSE will apply, on command from the central control, programmed stimuli at various inputs of the READI electronics. These stimuli will be distributed to the proper test points within each stage. GSE will then receive and condition the malfunction indicator, decision, and other selected responses from READI for transmission to the central control facility. GSE must provide its own switching for this READI computer test, preferably external to the stage so that when GSE is unplugged just prior to launch, the test circuits are open ended. In the event of a READI computer failure prior to launch, ground control will have the perrogative of replacing the computer or electrically deactivating the malfunction-decision channel which has failed from the system.
- Go, No-Go transducer status signals will be continuously generated and supplied to GSE by the READI self-check circuits.

The degree to which GSE and READI contribute in the evaluation of propulsion status will vary with the checkout phase. Beginning with the stage contractor's plant and up to the final countdown, GSE will control the monitoring of propulsion status. The READI system will provide both raw and processed propulsion data to GSE either through direct umbilical connection or the telemetry link. When the final countdown

commences and GSE carry-on or booster vicinity equipment phases out, emphasis will be shifted to READI to provide the necessary data to central control through telemetry. During the firing and liftoff phase, data transmission from READI to telemetry is considerably increased. After a brief period from the time the engines are fired, READI then assumes its primary function of automatic, propulsion monitoring.

The READI system can be designed with virtually no decrease in reliability to make a significant contribution to the simplification of GSE equipment and procedures. One of the major GSE design problems is the bandwidth limitations imposed in transmitting data over long cable lengths to the GSE test station. To solve this problem, the telemetry link is used to transmit the high response and precise data required by GSE. This necessitates additional on-board telemetry signal conditioning and commutation equipment as well as special equipment and procedures in the GSE system to calibrate the telemetry link.

Since the READI system contains electronic functions which are characteristically similar to many ground support checkout concepts, it can readily be adapted through suitable programming by GSE to perform some of the GSE data processing functions. The greatest advantage is realized if the data generated by READI is unaffected by fidelity deterioration incurred in the transmission to a remote facility. It is anticipated, therefore, that such data would primarily consist of Go, No-Go signals generated with various accuracies. This type of data also eliminates the need for calibrating FM and PAM telemetry systems. Data can also be provided to GSE in digital word form through a PCM telemetry system. The interface and trade-off potential between PCM telemetry and READI is discussed in paragraph C of this Appendix.

It is estimated that very little additional equipment would be required in READI to accommodate the propulsion data processing requirements of GSE. Some of these requirements may be satisfied by existing transducer signal comparator circuits, except that different reference levels may have to be generated. The main instrument of GSE-READI integration is the serial digital computer and associated input-output conversion equipment recommended as part of a hybrid READI computer. The versatility of digital sampled data techniques is outlined in Appendix C; it is an important merit factor in both the evaluation and design of the READI computer. The digital computer can be programmed to perform the necessary GSE functions and is operationally compatible with external GSE control of its program. The computer capacity which can be allocated for GSE integration is quite large during ground checkout.

It is recommended that the possibilities in GSE equipment simplification as afforded by READI be jointly investigated by the GSE and READI contractors as part of a cooperative study effort.

C. TELEMETRY/GROUND CONTROL-READI INTERFACE

The possibility of integrating the on-board parts of the telemetry and the READI equipment should be one of the first areas of study when investigating consolidation of launch vehicle systems. Since approximately 350 propulsion data signals on a three-stage Saturn are of interest for both telemetry and READI, it is reasonable to expect some overlap between the two systems.

Since there is a multitude of telemetry systems including PAM-FM-FM, FM-FM, UHF, PCM-FM and other types currently in production or development for advanced NASA vehicles, it is beyond the scope of this report to suggest any general or specific solutions to the integration problems. The advanced PCM telemetry systems currently under development offer perhaps the best opportunity for maximum integration with READI. It is unlikely that many of the analog signals conditioned by READI can be effectively used by the other telemetry systems. However, special uses of PAM and FM telemetry systems can be conceived where two-state binary data is processed by the telemetry system into two distinct pulse amplitudes or frequencies. The reasons for transmitting propulsion data in conditioned 1, 0 form are much the same as that outlined in the preceding GSE-READI interface section. The basic objective is to eliminate errors associated with the transmission of absolute values of a variable. In addition, reductions can be made in the number of high-response signal transmissions, such as vibration,which ordinarily require an excessive number of r-f links.

Designing PCM and READI systems so that they time-share or profitably utilize the same equipment blocks creates some functional conflict, such as the synchronizing of the READI computer program with time-dependent telemetry cycles. The hybrid, analog-digital candidate computer system recommended for READI development is quite compatible with digital PCM data handling. The components most likely to be involved in the effort to integrate and eliminate duplication in the PCM-READI systems include digital input gates, analog input gates, sample and hold, A/D converter, and digital storage. The use of the same signal gates is probably the simplest integration to accomplish. Integration of PCM and READI at a level higher than gating would markedly increase the synchronization and time-sharing problems common to both systems. In evaluating various consolidation possibilities, the loss of certain operational features must be balanced against

achievable cost and weight savings. It will be appreciated that the need for such integration would be strengthened if the READI-PCM systems were being developed concurrently.

Figure D-1 broadly illustrates the functional tie-in of READI to telemetry. A separate telemetry system is assumed for each stage of the launch vehicle. The following READI system information is recommended for r-f transmission to the central control facility:

1. Raw Engine Data

This will be obtained directly from the READI transducers or signal conditioner outputs. This data will be used for a more thorough evaluation of the propulsion system performance by large capacity, ground-based digital machines, perhaps within a framework of operational flight control. It is expected that all such data will be recorded.

2. Transducer and Computer Status

Transmission of READI status information to ground control may be useful for improving the performance of the vehicle-ground monitor loop. The situation can be conceived where a failure in READI is detected by ground control and appropriate override action exercised. The transducer and computer status information is generated by the READI self-check circuits.

3. Malfunction Indications and Decisions

The effectiveness of ground control monitoring is greatly enhanced by providing ground control with the malfunction indicator and decision outputs of READI. One scheme which merits consideration would be to at least duplicate the READI function on the ground as a check on READI performance. The relative reliabilities of the on-board and ground loop would have to be evaluated before an operational scheme of this type can be developed.

D. GUIDANCE AND CONTROL - READI INTERFACE

The guidance and control system is the major instrument of on-board mission control. For the type of three-stage vehicle studied, the computer for this system is assumed to be a general purpose digital machine which can be programmed to accommodate a variety of missions. An adaptive guidance system is assumed which derives position/velocity data and computes an appropriate tilt program and engine cutoff commands. The control system provides for vehicle attitude control and stability through the gimballed engine nozzles.

The guidance and control-READI interface, although minor in the extent of wiring, is functionally quite important. Four major input-output data requirements were hypothesized.

1. READI Outputs to Guidance and Control

a. Engine Control Decisions

All READI decision outputs will be transmitted to the guidance system. Rapid, unambiguous indications of engine shut-down or other modifications to engine operation provide anticipation for more effective guidance control and stabilization during these thrust transients. Without this information the guidance system must rely on its body-fixed longitudinal accelerometer in conjunction with other information to sense thrust irregularities after they have occurred.

b. Fuel/Oxidizer Mass Flow Rates

The minimization of propellant consumption is an important adaptive guidance parameter, particularly during an earth rendezvous operation. For fixed-thrust engines, guidance optimization of this parameter is based on an assumed constant flow rate, thereby reducing the problem to a condition of minimum propelled flight time. Where the upper stage engines are throttleable, a more extensive fuel energy management function is required encompassing both minimum fuel and minimum time modes. Such a function would logically be implemented within the central mission computer and operate in conjunction with the guidance system. Since propellant mass flow rates change as a result of READI actions, this information will be supplied by READI to the central mission computer.

2. Guidance and Control Inputs to READI

a. Time-To-Go to Stage Separation

Time-to-go is continuously computed by the guidance computer to provide a cutoff signal to the stage separation system. The availability of this information permits the possibility of devising some predictive concepts in engine malfunction detection. These concepts are discussed in Appendix K. The use of time-to-go as a parameter in an automatic abort system is treated in paragraph F of this Appendix.

Another concept involving the use of time-to-go information in READI relates to the inhibiting of certain decisions when stage separation is approached. This concept is based on analyses which indicate

that for certain malfunctions the risk associated with not taking corrective action decreases as time to stage separation decreases. These malfunctions are restricted to those with virtually zero explosion hazard and include:

- Loss of helium (#1)
- Low pump speed (#6)
- Loss of electrical power (#9)
- Low fuel flow - all engines (#19)
- Low oxidizer flow - all engines (#31)

The inhibiting of decisions resulting from these malfunctions is particularly important during the terminal phase of a critical maneuver such as orbital insertion; it is desirable to avoid thrust vector disturbances if possible. It is very probable that the time-to-go values programmed for decision blanking would be different for each malfunction. The implementation of this concept is quite simple, and there is no compromise in READI reliability.

b. Vehicle Attitude Rates

Three-axis attitude rate signals are required from the guidance and control system if READI is designed to include the abort sensing and initiation function described in paragraph F of this Appendix.

E. PROPELLANT UTILIZATION - READI INTERFACE

The propellant utilization system functions to regulate the O/F flow ratio to insure that neither oxidizer nor fuel is depleted before stage separation. Closed loop control of relative propellant quantities is normally exercised by positioning a valve in the oxidizer line of each engine. The valve servo is normally limited in authority within an acceptable range of O/F operation. For the model second stage engine studied, an O/F band of 4.5 to 5.5 is assumed.

Since the control of oxidizer flow rate by the propellant utilization system directly affects the constants of several READI malfunction indicator equations, proportional servo position information is required. This information is transformed into an O/F quantity and the equation constants modified in accordance with open-loop schedules.

F. ABORT SENSING AND INITIATION

The hazardous nature of many cryogenic propulsion failures suggests that mission abort be programmed as an alternate READI action. Because of the extensive and intricate timing-interlocking functions required between the various systems associated with the abort

procedure, a central, automatic abort sensing and initiation system warrants strong consideration. Since the engines are the cause of approximately 60 percent of the major vehicle failures which lead to abort, it is logical to consider including this function within READI. It is to be noted, however, that the actual abort function is not implemented in the model READI system described in this report.

For vehicles of the type considered in this investigation, it is estimated that the abort sensing requirements will be largely predicated on the hazardous conditions of operation described below. These conditions reflect failures in the key propulsion and control/stabilization systems. Aborts necessitated by failures in other vehicle systems will be implemented by other means.

1. Multi-Engine Shutdown

A simultaneous or sequential multi-engine shutdown can result from multiple propulsion failures within the engines or stage. It is quite probable that abort initiation due to multi-engine shutdown will be time dependent. To formulate this time function in the abort computer program, information on propulsion performance is required from the stage and engine contractors.

2. Explosion Within an Engine or Stage

Although an explosion within an engine or stage is quite improbable with a perfectly functioning READI, the sensing of such an event and initiation of an immediate abort is vital to crew safety.

3. Rapid Loss of Tank Ullage Pressure

A potentially hazardous condition is indicated by a rapid loss in tank ullage pressure. The danger associated with such a failure depends largely on the structural characteristics of the vehicle stage. There is associated with each stage a minimum tank pressure that must be maintained if structural integrity of the vehicle is to be realized, particularly in the region of maximum dynamic pressure flight. The sensing function conceived for tank burst failure is

$$p + \frac{dp}{dt}(\Delta t) > P_m$$

where p = tank ullage pressure

p_m = minimum allowable pressure

t = time-to-go to stage separation.

Rate anticipation is deemed necessary to affect a successful abort before a collapse of the vehicle structure. Some filtering may be required in the predictive term of the equation shown previously to attenuate higher frequency variations in pressure.

4. Over-Limit Vehicle Attitude Rates

Monitoring of vehicle attitude rates in all three axes is an excellent indicator of control and stabilization system performance. It has been successfully applied in on-board abort systems for many launch vehicles including Mercury-Atlas. For a multi-engine stage vehicle, it is estimated that a single never-exceed limit would be required in each axis for each stage of flight. The attitude rate data would be supplied by the guidance and control system.

The initiation of automatic abort action by an on-board computer involves some special considerations. In most instances the first step in an abort procedure is an immediate all-engine shutdown. For manned flight this is followed by stage separation and capsule ejection. Ground control is informed through the telemetry link for rescue and range safety purposes. Unmanned flights may reflect somewhat different abort procedures based on range safety considerations (see paragraph G below).

In addition to its self-generated abort command function, it is desirable that the abort computer shut down the engines in response to both ground control and crew abort signals. By directing these commands through the central abort computer, the manual-automatic interface problem is simplified, and maximum reliability ensured. The decision logic and engine control section of the READI computer can be easily modified to accommodate this interface and provide the super-reliability required for all-engine shutdown..

G. RANGE SAFETY

The model READI system described in this report can be functionally modified to provide compatibility with launch site operational procedures. Range safety is one operational factor which may impose a number of special functions or constraints on READI. For example, an engine shutdown on the Mercury-Atlas vehicle is not permitted until 30 seconds after liftoff. It is conceivable that a similar constraint may be placed on READI in larger boosters, such that actions cannot be initiated until an arming command is relayed after some elapsed flight time. Thus, because of range safety considerations an increased mission risk may have to be assumed during this interval of time. During this initial phase of flight READI could provide ground

control with computed indications of malfunction, in addition to raw engine data through the telemetry system. The ground controller would exercise decision control through the radio command link.

An abort procedure under consideration for multi-stage vehicles such as Saturn includes a programmed shutdown of selected engines so as to direct a malfunctioned vehicle to an ocean area. In addition to thrust vector control, such a procedure would involve a computer program of selected engine shutdown and thrust uprating which can be accomodated in the decision logic section of the READI computer.

D-3. INSTALLATION

A. INTRODUCTION

The installation of a READI system will necessarily depend on the stage for which it is designed. A preliminary examination of several real stages, however, reveals the possibility of two basic approaches to the READI computer installation and packaging designs. The engine transducer installation is the same in each case. The first approach provides for a single electronic package comprising all the READI functions and strategically located in close proximity to the stage test panels and cable tunnel. The scheme envisioned in the second approach would provide a separate unit for each engine comprising those circuits peculiar to each engine. These units are mounted relatively close to the engines and include parallel signal conditioning and malfunction detection, transducer self-check, and switching circuits. The digital arithmetic, input-output conversion, decommutation and storage, decision logic, and other circuits common to all engines are contained in a central unit. This central unit, as in the first approach, would be installed so as to minimize the wiring interface to other stage and vehicle systems.

Rather bulky, fire-resistant wiring is required for transducer connections independent of the installation approach. To minimize weight, this wiring is terminated at engine test panels mounted on the stage frame outboard of the engines. The interconnection between these panels and the READI computer can be accomplished with lighter weight wiring.

It is recommended that all READI electronics be mounted to the stage frame and off the engines. This will require some flexibility in the cabling to accommodate the gimballed motion of the

engines. From the standpoint of environment and cabling, the installation of READI computer electronics between the heat shield and propellant tanks appears to be optimum.

B. EVALUATION OF INSTALLATION APPROACHES

The merit of each installation approach is discussed below for a number of evaluation factors. A firm recommendation cannot be presented without a more thorough study of real stage designs.

1. Accessibility

Accessibility of the READI electronics during the various checkout phases is an important consideration in the READI installation design. The single-package approach appears to present no accessibility problem. A problem may exist, however, in the multi-package approach if sufficient access ports around the periphery of the vehicle are not provided, or if the vehicle stand configuration restricts the ability of ground personnel to replace any one unit.

2. Electrical Pickup

The multi-package approach warrants strong consideration because of the noise pickup problem. By processing the raw engine data signals within 8 to 10 feet of the engine transducers, the noise interference problem is considerably less than that encountered in the single package design. The latter approach requires transmission of engine data signals in much longer wiring routed in a large circular pattern around the engines to the central computer unit. With respect to the multiplexed analog signals emenating from the separate engine modules, shielding may be required to preserve fidelity of transmission. In any case the shielding of a single lead is a much simpler problem than shielding the large bundle of wires required with a single computer package.

3. Environmental Effects

The multi-package approach inherently required more extensive provisions for temperature, pressure, vibration, and other environmental controls than a single, integrated computer unit.

4. Weight

There is no appreciable difference in weight between the two installation approaches. The higher weight associated with the

shielded cable requirements of the single package approach is almost offset by the higher chassis weight incurred in multi-unit design.

5. Volume

Indications are that no volumetric constraints will be encountered with either installation approach for any single or multi-stage vehicle.

Appendix E

DESCRIPTION OF A SECOND STAGE READI SYSTEM

Appendix E

APPENDIX E

DESCRIPTION OF A SECOND STAGE READI SYSTEM

E-1. INTRODUCTION

The hybrid system selected for READI in Appendix C is an advanced design based upon the use of microelectronic circuits to increase reliability. The design allows the system to be versatile, flexible, and highly reliable while reducing the cost to a minimum.

The READI system is composed of two major function subsystems:

- Continuous parallel-wired malfunction-to-decision channels
- Serial digital computer.

These subsystems are miniaturized, microelectronic circuits providing low false alarm and missed alarm probabilities. A self-contained continuous and programmed checkout of the transducers and computer is provided to reduce the possibility of false alarms. Continuous self-check of the transducers is employed in the parallel-wired channels and a programmed self-check of the transducers and computer is provided by the computer program.

E-2. SYSTEM DESCRIPTION

The continuous malfunction-detection channels provide continuous data with high reliability, where simple functions are defined. The complex functions are sequentially processed by an analog-to-digital converter and digital computer. An investigation of the computing and data handling requirements of the READI system indicates that a serial machine can handle the requirements and still have excess capacity for growth. In addition, the simpler organization of the serial machine results in a few components, thus improving the weight, volume, power consumption, and reliability.

A block diagram of the proposed second stage READI system is shown in figure E-1. The continuous malfunction-detection channels and storage units provide continuous parallel-wired channels

for the simple functions, utilizing microelectronic circuitry. The parallel-wired channels normally employ simple signal conditioning and digital logic circuits. A detailed description of these circuits appears in a later paragraph of this appendix.

The serial digital computer processes the complex functions, time-sharing the computers serial arithmetic unit and memory. Two memories are used:

- a wired permalloy core program memory
- a data memory using permalloy cores for the fixed memory and bi-aperture ferrite for the alterable memory.

The data word consists of 11 bits, including sign and parity; the program word consists of 15 bits.

A five-bit command structure provides 32 commands, allowing for the future expansion of the computer. A summary of the computer characteristics is listed in table E-1. A detailed description of the serial digital computer is covered in a later paragraph of this appendix.

TABLE E-1

COMPUTER CHARACTERISTICS

Organization	Serial: whole number
Number System	Binary: two's complement
Circuitry	Microelectronics: permalloy and bi-aperture ferrite memories
Bit rate	0.5 megacycle
Word length	12 bits
Precision	11 bits including sign and parity
Computing capacity	
Data processing	24 us
Add or subtract	24 us
Multiply	288 us
Divide	312 us

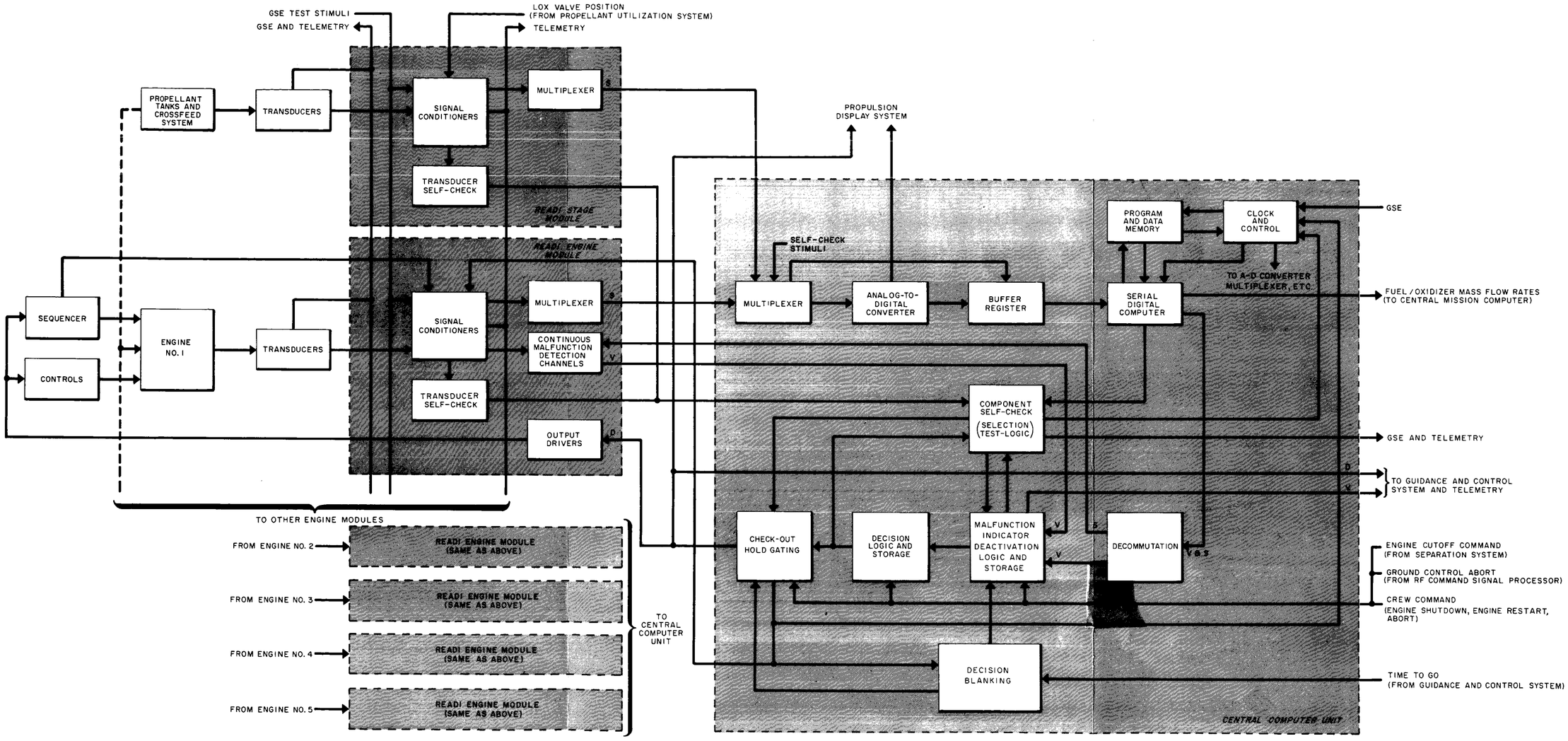


FIGURE E-1
SECOND STAGE READI SYSTEM BLOCK DIAGRAM

TABLE E-1 (Cont)

COMPUTER CHARACTERISTICS

Storage Capacity	
Program	512, 15-bit wired words; serial readout
Data	64, 11-bit, word organized memory non-volatile, non-destructive serial readout; electrically alterable
	128, 11-bit wired words; serial readout

A. SERIAL DIGITAL COMPUTER

1. Command Structure

All commands with the exception of "Multiply" and "Divide" require one word time to execute. Multiply requires (n) word times and divide requires (1 + n) word times which, for 11 bits of precision, becomes 11 and 12 word times respectively.

2. Arithmetic and Control Unit

a. Circuitry

The arithmetic and control electronics will consist of microelectronic circuits throughout. The basic circuit speed has been specified at 200 nanoseconds in order to achieve a 0.5-mc (2000 nanosecond) operating speed with maximum assurance. A description of the microelectronic circuits appears later in this appendix.

b. Operational Registers

The computer operation, figure E-2, can be visualized readily by considering the functions of the basic operational registers.

- Next Instruction Address Counter - Ten bits are used to address the program memory. The number in the register is updated every word time. During program transfer commands, the contents of the next instruction address counter are replaced by the contents of the address portion of the next instruction register.

- Next Instruction Register, 15 bits - This register receives the computer instruction word from the program memory in serial form. At the beginning of an operation, the five-command bits of the instruction word are transferred to the command register. The address portion of the instruction word is transferred to one of two places.
  - To the next instruction address counter during program transfers.
  - To the data memory address register for all other commands.
- Command Register, 5 bits - This register contains the command being performed by the machine. The ten-output leads of this register are matrixed to produce the 32-command lines which operate the control unit.
- Data Memory Address Register, 8 stages - This is a microelectronic register containing the decoded address of 1 out of 128 fixed or 64 alterable words in the data memory.
- Program Memory Address Register, 32 stages - This is a microelectronic register containing the decoded address of 1 out of a possible 512 program words.

c. The Arithmetic Unit

The arithmetic unit is composed of microelectronic circuitry operating at a 0.5-megacycle rate. All arithmetic operations in the computer are performed serially.

The major units of the arithmetic unit consist of the accumulator, add-subtract unit and register.

3. Program Memory

a. General

Control of a digital computer can be accomplished by one of two methods:

- Control of the computer arithmetic through a stored program
- Control of the computer arithmetic through a wired-in form of program.

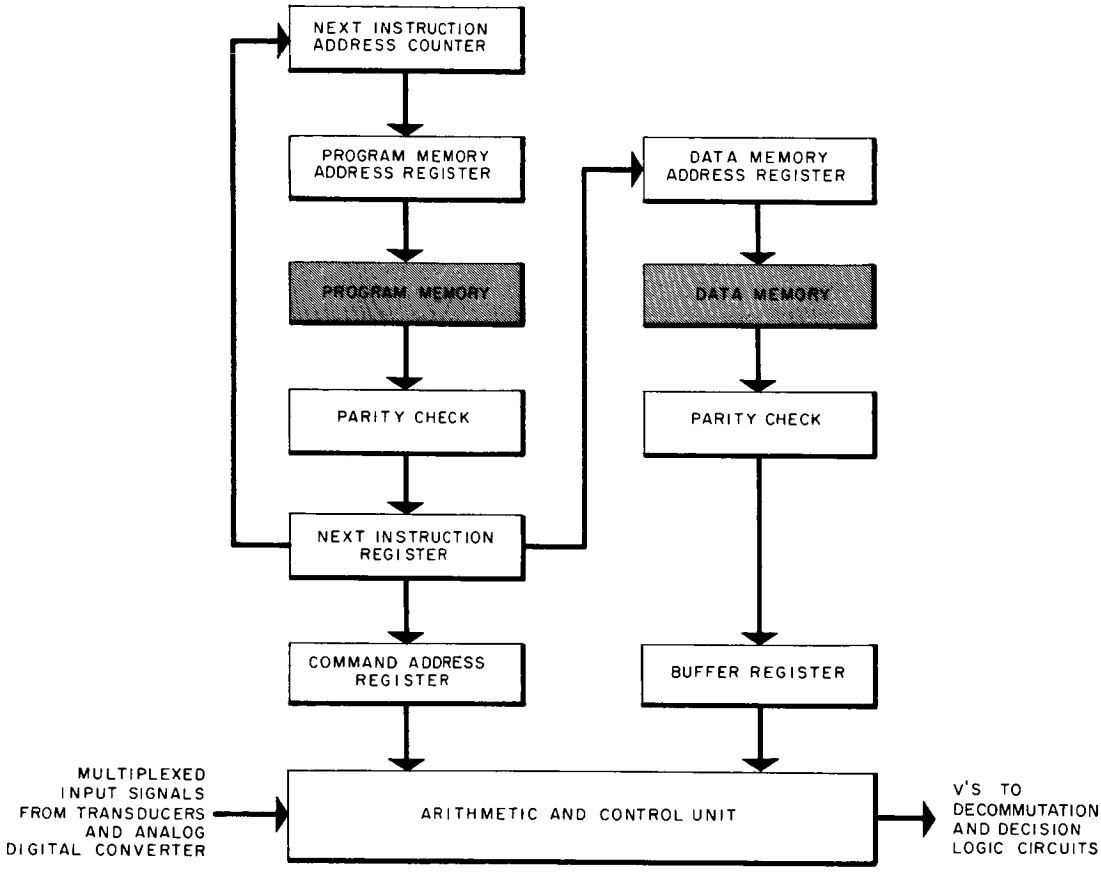


FIGURE E-2
DIGITAL COMPUTATION
BLOCK DIAGRAM

The stored method uses stored numbers which are coded to indicate the operations desired in the computer. Under control of a sequencing device, these coded numbers are selected, decoded, and outputs are developed for use in the internal logic circuitry of the computer. The stored program method of computer control is flexible, and computer operation can be readily changed by modification of the stored numbers or words. For this reason, the stored-program method is normally used in general type machines where maximum operational flexibility is a prime requisite. The stored-program control requires considerable hardware for its implementation.

For more specialized applications, where flexibility is secondary and simplicity of hardware is prime, a wired-in type of program control is usually employed. Examples of applications of this type are missile guidance and launch computers. Use of this type is clearly indicated for READI, too. The wired-in type of program control is simple and does not require as much hardware as the stored-program method. The "rope" or wired memory was selected since it provides:

- Considerable savings in hardware, more reliability, and more compatibility with redundancy techniques. Redundancy can be applied without excessively increasing hardware complexity. In addition, the basic program information is carried by physical wiring and is not susceptible to circuit parameter changes.
- High-bit density
- Non-destructibility in field use
- Ease of change in engineering test
- Low cost
- Short lead time to provide a new memory if new functions are added to the computer
- Non-volatility
- Wide temperature operation.

b. Wired-Program Memory

The wired program uses tape-wound permalloy cores as the storage medium. The memory stack consists of a matrix, 8-cores wide and 15-cores deep. The 8 cores in the first row of the matrix store the first bits of all the words in the memory. The second row stores the second bits, and so on through 15 bits. Figure E-3 is a pictorial diagram of a simplified wired program.

The functions of the wires in reading the memory matrix are four in number:

- The 8 Y-set lines select one out of 8 columns of cores and switch (set) all 15 cores in the selected column.
- There are 64 possible X-paths (inhibit lines) consisting of 64 X wires arranged to pass through all 15 rows. Each of the 64 X wires may or may not pass through a particular core in the memory matrix depending on whether a one or a zero is to be stored in the core for that particular word. Thus, each core in the matrix represents 64 bits of information. (There are 8 columns of 15 bits each. Therefore, the memory consists of 64 x 8 or 512 15-bit words.)
- A single clear wire is threaded through every core in the memory matrix.

Several advantages are apparent in the proposed technique:

- It is not necessary to matrix the output of groups of sense wires in order to select one group from the others. This is particularly important because the sense wires are susceptible to electromagnetic pickup. Adding selection circuitry to the circuits increases the effective loop area of the wires and thus compounds the problem of noise.
- The proposed technique is adaptable to serial readout and requires one sense amplifier in the present application in contrast to 15 sense amplifiers required for parallel readout.

4. Data Memory

a. General

The data memory, figure E-4, is a 128-word, 11-bit, wired-in type, identical in operation to the program memory and a 64-word, 11-bit word-organized memory which uses bi-aperture ferrite elements as a storage medium. Micrologic steer circuits, similar to the program memory steer circuits, are used to select the desired word and to clear a word prior to writing new information into the alterable memory. Also, as in the program memory, a sequential switch reads the memory one bit at a time.

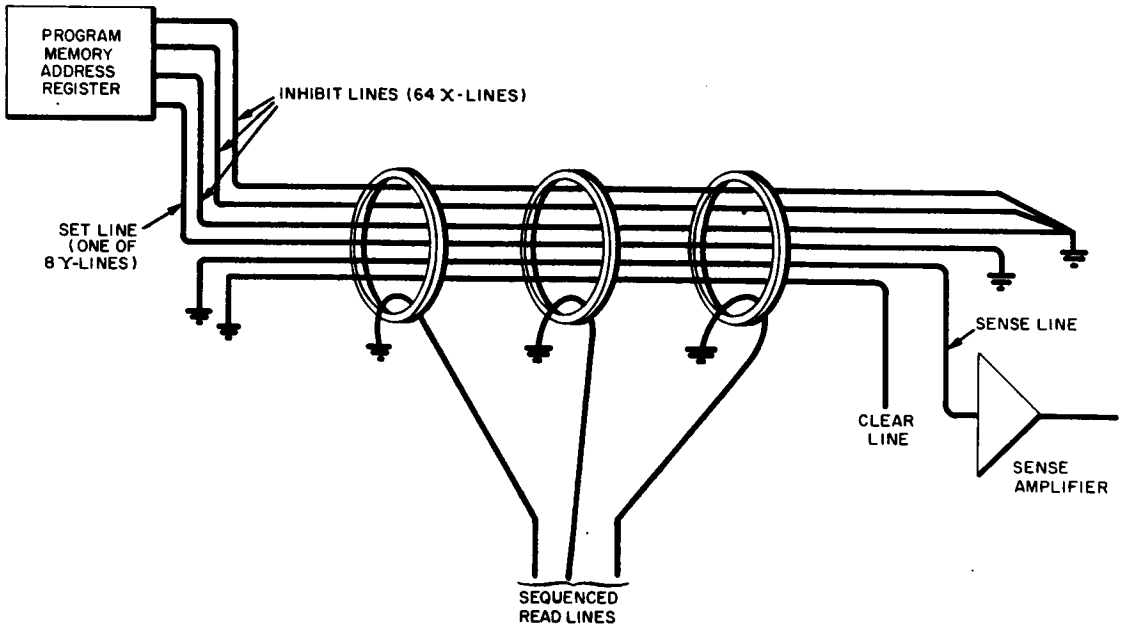


FIGURE E - 3
SIMPLIFIED WIRED PROGRAM

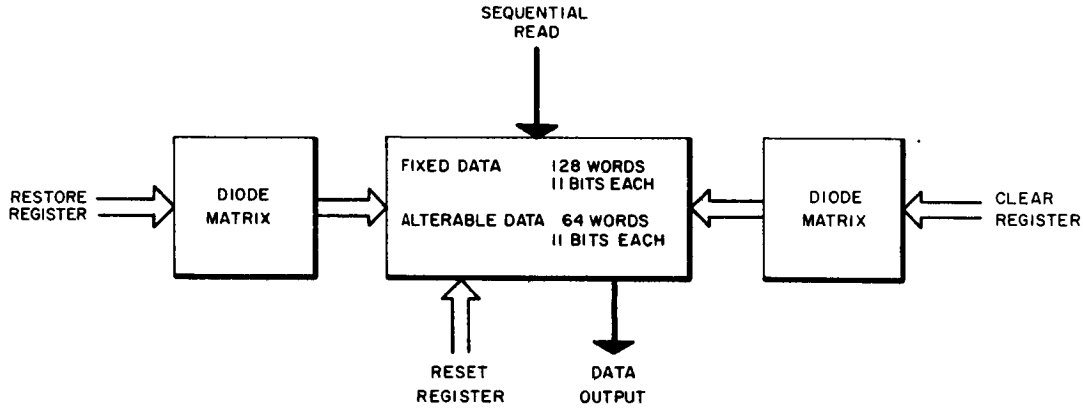


FIGURE E-4
DATA MEMORY

b. Alterable Memory

The bi-aperture element has the advantage of having non-destructive readout (NDRO) properties. In the proposed memory, it is not necessary to rewrite information after it has been read, unless it is desired to change the information in the memory slot. Thus, unlike single aperture memory systems which are DRO (destructive readout), the bi-aperture element (NDRO) achieves the maximum reliability in data handling because information is never lost in transit due to power transients.

The alterable data memory is organized to take advantage of the fact that the bi-aperture element has three possible states:

- zero
- primed one
- unprimed one.

The element cannot be read unless it is in the primed state. In other words, a pulse of current on the read line results in zero voltage on the sense line if the element is in either the zero state or the unprimed one state. Only when the element is in its primed one state will a read pulse produce a signal on the sense wire, and the read pulse restores a primed one to an unprimed one.

The element can be changed from its one state to a zero state by the coincident application of prime and read pulses. However, unlike conventional single aperture memory systems, a pulse of current on the read line or the prime line can be arbitrarily large without destroying the information.

B. MULTIPLEXER AND ANALOG-TO-DIGITAL CONVERTER

A block diagram of the major functions of the analog-to-digital voltage converter unit is shown in figure E-5. In system operation, data are always available at the input to the multiplexer. At predetermined points in the computer program cycle an external function command signal is generated and addressed to the multiplexer unit. Each line selects a specific data channel and causes a sampled value of analog data to be transferred to the analog-to-digital converter and buffer register. Some input signals, which are already in binary form, are gated directly to the buffer register.

1. Analog-to-Digital Converter

The following voltage converters were considered in the selection of a voltage encoder.

a. Range and Staircase Method

These are indirect voltage-to-digital techniques in that the voltage is first converted to a time interval and then to digital form. In addition to the circuits necessary for time conversions, a comparator and ramp or staircase generator is necessary. Even though this method can be multiplexed, the relatively long conversion time prevents it from being heavily multiplexed.

b. Cascade Stages Method

This is a method for converting a voltage to a digital number by succession comparisons and subtractions. It consists of a number of iterative stages determined by the precision required. At each stage the input voltage is compared with the reference voltage and then on the basis of comparison, either a 0 or 1 is read out. This method has a relatively short conversion time. However, the logic is complex and requires a relatively large number of components.

c. Continuous Balance Method

This is a feedback method which uses a digital-to-analog converter in the loop. The output of the digital-to-analog converter is compared with the analog input signal. The resultant error signal is clamped and used to control the direction in which the forward-backward counter is stepped. This method is relatively slow, requiring a conversion time essentially the same as that for the ramp-method.

d. Successive Approximation Method

This is another feedback method and is the basis of operation for the capacity encoder. Although it makes a complete new measurement each time digital data is sampled, it requires only n steps to complete the measurement as compared to the 2n-1 steps required for the ramp or staircase and continuous balance method for an output having n bits. Also, this converter lends itself well to time-sharing techniques, and only a minimum of control circuitry is required to switch from one analog input to another. A functional block diagram of the capacity encoder is shown in figure E-6.

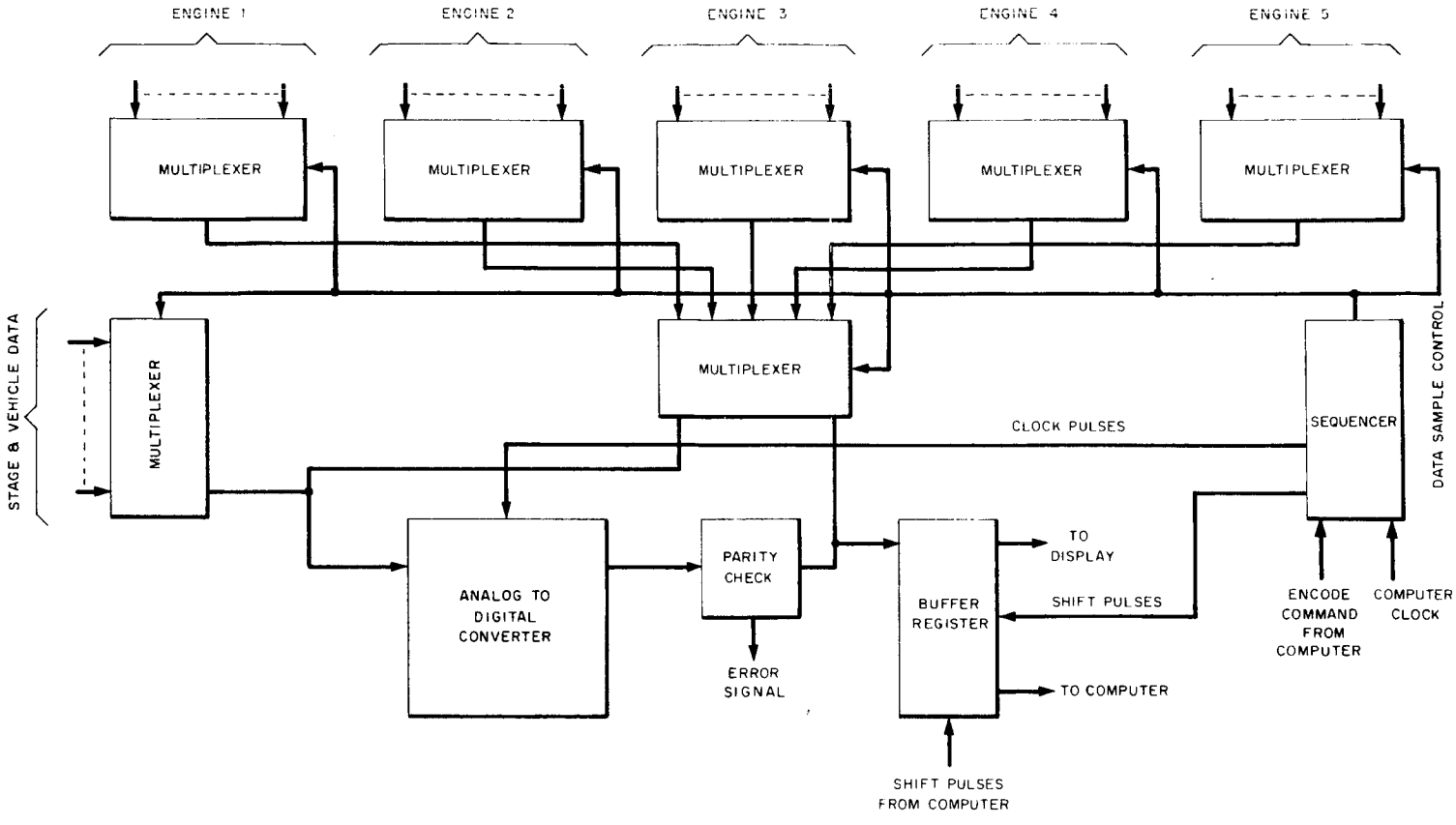


FIGURE E-5

MULTIPLEXER AND
ANALOG-TO-DIGITAL CONVERTER

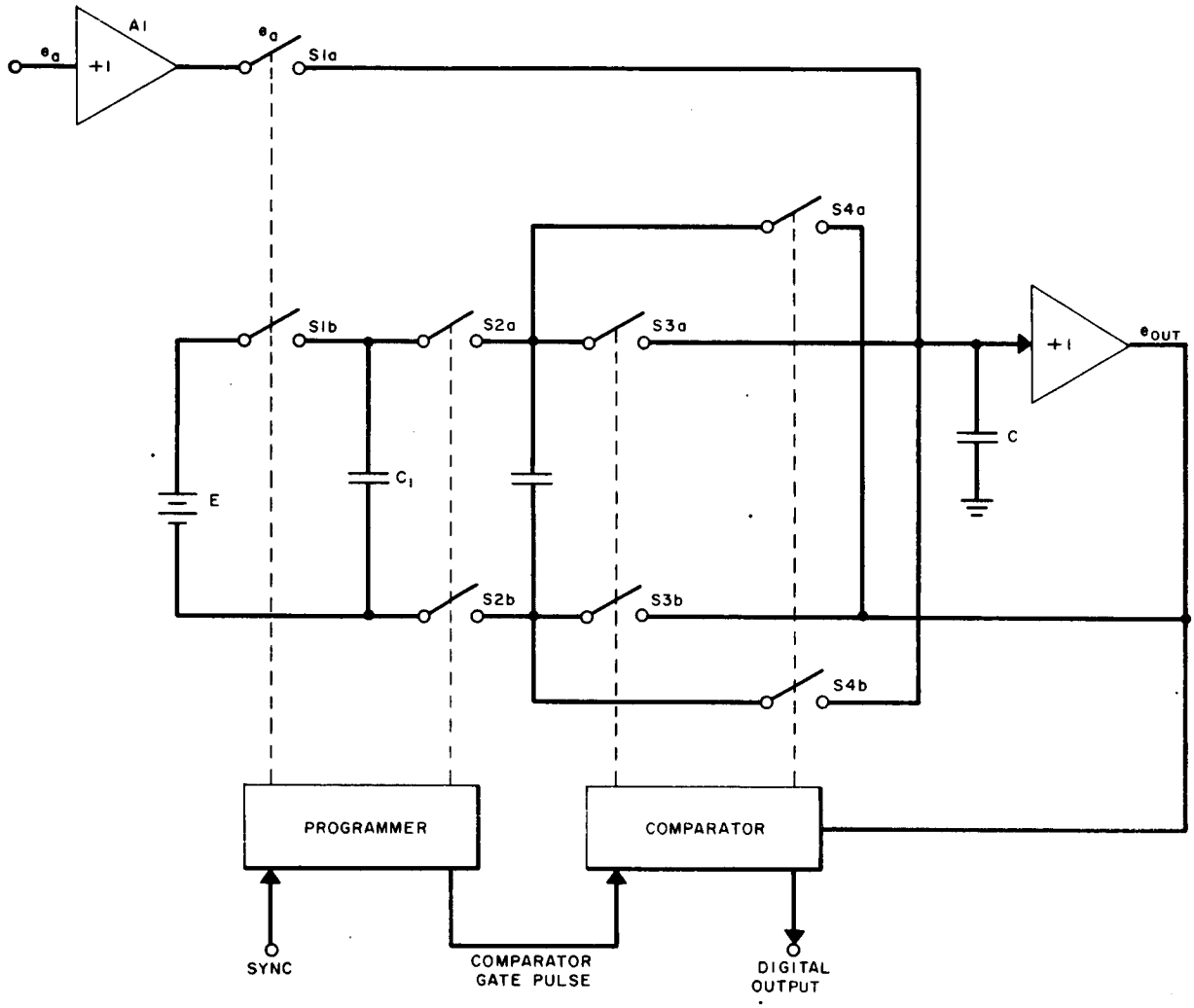


FIGURE E-6
CAPACITY ENCODER

2. Multiplexer

The large number of analog input signals to the digital computer dictates a time sharing of the converter in order to maintain a reasonable cost, size,and weight for the input conversion equipment.

In all the multiplexers considered, an electronic switch was used for the switching of analog voltages. The difference between the various schemes is the complexity of the circuits required to normalize the input signals and the fidelity of the switched signals. The capacity multiplexer was found to have a switching fidelity comparable to other multiplexing methods, while using the least number of components. The capacity multiplexer is a device for commutating electrical signals by the use of electrical charge transfer techniques. Each of the analog input signals charges an input storage capacitor to the potential of the corresponding input signal, and the resulting charges are transferred in sequence to an output capacitor in the encoder.

A functional block diagram of the capacity multiplexer is shown in figure E-7. The multiplexer has the ability of switching single-ended and double-ended inputs and providing the appropriate individual channel gains by the selection of C_n. The expression for the desired channel output voltage, e_o, is

$$e_o = \frac{C_n}{C} e_n$$

As with all multiplexing systems, the multiplexed signal must be filtered if the information perturbations exceed the sampling rate. Input voltage e_3 illustrates how a resistor (R_3) may be utilized to attain the required time constant.

3. Conclusions

The analog-to-digital converter and multiplexer units which utilize the simplest and most reliable circuits at the least cost are the capacity multiplexer and encoder. The predicted failure rates of these units are:

Capacity encoder - failure rate of 1×10^{-4}

Capacity multiplexer - failure rate (per switch) of 0.05×10^{-4}

Therefore, the capacity encoder and multiplexer were chosen as the units to be used in READI.

C. CONTINUOUS MALFUNCTION DETECTION CHANNELS

The continuous malfunction detection channels are implemented where simple functions are required. The second stage READI block diagram, figure E-1, illustrates this subsystem which may be broken down into two logical areas for discussion:

- Signal conditioners
- Logic circuits.

1. Signal Conditioners

Two main types of signal conditioning circuits are used in READI:

- Transformation of the raw sensor data into a two-state binary form; that is 1 or 0, representing two discrete regions of the measured parameter
- Modification of the electrical characteristics of the transducer output to provide signals compatible with the multiplexer requirements.

Figures E-8 and E-9 illustrate two signal conditions which provide a 0 to 1 state output. The 0 state represents the engine under normal operation, while the 1 state indicates an abnormal engine condition... The reliability of each circuit is specified for both modes of failure; λ_m is the missed alarm failure rate and λ_f is the false alarm failure rate.

a. Phase Sensitive Switch

The signal conditioner illustrated in figure E-8 senses the state of a single-coil variable-reluctance transducer. The transducer is used to sense the position of a two-state hard-over position, i.e., valve position. The transducer is balanced in an a-c bridge circuit at approximately the mid-point of travel. The demodulator senses the phase of the transducer output and activates the Schmitt trigger to produce either a 1 or 0 output, as required.

b. Polarity Detector

The polarity detector circuit is illustrated in figure E-9. The transducer is balanced in a d-c bridge circuit at the selected threshold value of the variable. The output voltage polarity of the bridge network will change as the variable passes through this

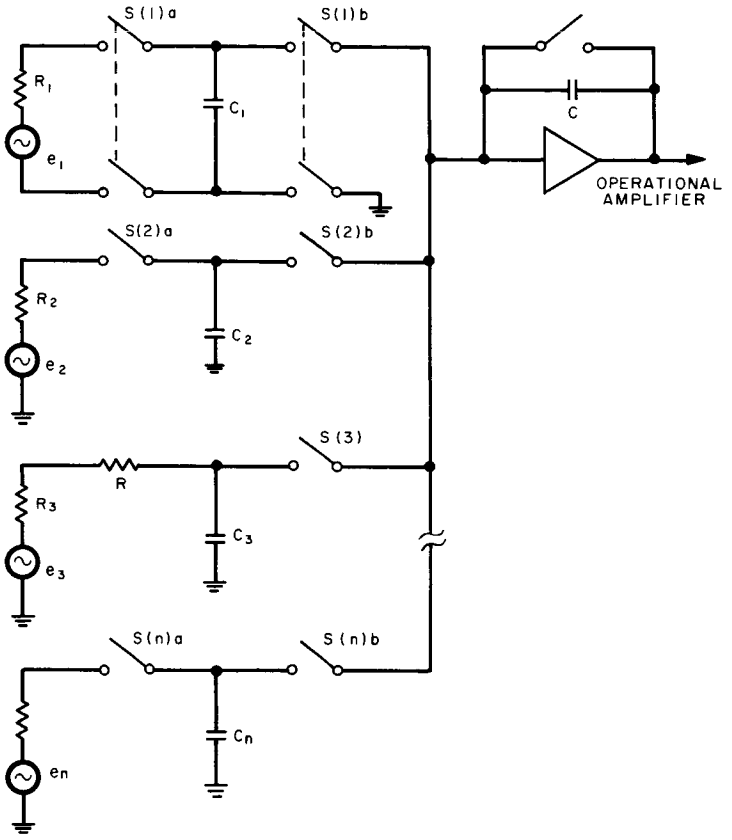


FIGURE E-7
CAPACITY MULTIPLEXER

TYPICAL SIGNAL CONDITIONER - SC 18

FUNCTION: Phase Sensitive Switch

INPUT: Voltage V_1

OUTPUT: $V_o = 0$ - Amplitude 0.25 to 0.4 volts

$V_o = 1$ - Amplitude 1.15 to 2.2 volts

SENSITIVITY: Change in state with a change in input signal phase

RELIABILITY: $\lambda_f = 0.02 \times 10^{-4}$

$\lambda_m = 0.1 \times 10^{-4}$

ACCURACY: —

SIZE: 0.74 $in.^3$

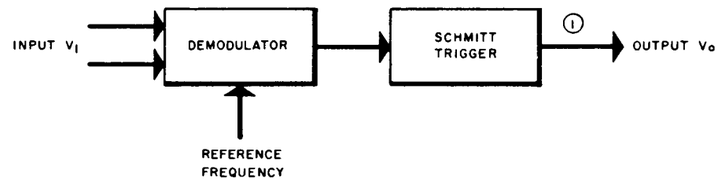
WEIGHT: 0.00616 lb

POWER: 30 mw

READI FORM NO. 2 Sheet 1 of 2

TYPICAL SIGNAL CONDITIONER - SC 18

CIRCUIT:



READI FORM NO. 2 Sheet 2 of 2

FIGURE E-8
TYPICAL SIGNAL CONDITIONER - SC 18

threshold value. The output voltage is then modulated and amplified before being used to activate a Schmitt trigger. The reference frequency to the modulator is also used to trigger a second Schmitt trigger which has a slight offset in its bias level. The outputs of the two Schmitt triggers are compared in a coincidence detector (AND gate), where an output will appear when the polarity of the bridge output voltage is correct. The reference Schmitt trigger has a shorter period of conduction than the signal Schmitt trigger and will eliminate false triggering on the leading and trailing edges caused by slight phase shifts between the two Schmitt trigger outputs. The output of the signal Schmitt trigger can incorporate an RC filter to prevent spurious coincidence output for small perturbations about the Schmitt trigger firing point.

The second type of signal conditioning circuit (figure E-10) converts the transducer proportional a-c input voltage into a d-c voltage. The incoming signal is amplified, demodulated, and filtered for use by the capacity multiplexer. The capacity multiplexer normalizes the input voltage by a capacitance transfer technique; therefore, the amplifier may be eliminated if the transducer input has a sufficient amplitude.

The circuits used for the signal conditioners are either microcircuits or thin film circuits. A complete description of these circuits appears later in this appendix. The microcircuits are complemented whenever possible and provide the highest reliability within the state-of-the-art. The thin film circuits are used where integrated circuits are not available and have a reliability comparable to that of the microcircuits, but are slightly greater in volume and weight.

2. Logic Circuits

The signal conditioners binary outputs (S_n (1, 0)) are gated through microcircuits which perform simple Boolean logic functions. Two types of circuits used are the AND gate and OR gate, depending upon the operations specified in the signal space separations, table A-2 in Appendix A. The signal element integrated circuit provide these required operations with a high degree of reliability. A description of these elements appears in the component section of this appendix.

D. DECOMMUTATION

The output of the serial digital computer is in serial form, therefore, gating is required to route the information to the

proper locations. This gating is performed by the decommutation circuits which are sequenced by the computer control. The output signals from the computer are either conditioned transducer signals (S_n (1,0)) or malfunction indicators (V_m (1,0)). The conditioned transducer signals are routed to the engine malfunction detection channels for further processing by the logic circuits, while the malfunction indicators are routed to the deactivation logic circuits and storage. Logic gates are used for decommutation, therefore, micrologic circuits are implemented for this function.

E. MALFUNCTION INDICATOR DEACTIVATION AND STORAGE

The malfunction indicator deactivation and storage circuit inhibits erroneous malfunction indicators and stores the valid indicators. The deactivation of specific malfunction indicators is triggered from three sources:

- External commands (ground control, crew, stage separation)
- Decision blanking
- Component self-check logic.

A detailed description of the external commands appears in Appendix D, while the decision blanking and component self-check logic circuits will be discussed later in this appendix.

The malfunction indicator deactivation circuits are simple AND gates which are normally enabled to pass the malfunction indicators through to the storage flip-flops. However, upon receipt of a deactivation signal the gates are disabled and the storage flip-flops are reset, inhibiting the malfunction indicator from entering the decision logic and component self-check logic. Reactivation is dependent upon the source of the deactivation signal. Some signals are disabled for a specific time period, while other signals are disabled permanently, as will be explained later in this appendix.

F. DECISION LOGIC AND CHECKOUT HOLD GATING

The decision logic consists of micrologic OR gates and output circuits. The malfunction indicators are routed through these OR gates to the output circuits which are capable of driving the required engine controls to perform the indicated decisions. However, the checkout hold gating is capable of inhibiting the decisions upon commands from three sources:

TYPICAL SIGNAL CONDITIONER - SC 21

FUNCTION: Polarity Detector

INPUT: Bipolar Analog Voltage (V_s)

OUTPUT: V_o = "1" For input $V_s > o$

V_o = "O" For input $V_s \leq o$

RELIABILITY: $\lambda_f = 0.14 \times 10^{-4}$

$\lambda_m = 0.44 \times 10^{-4}$

ACCURACY: ±5% (Dependent on Amplifier Gain Allowable)

SIZE: 2.2 $in.^3$

WEIGHT: 0.0172 lb

POWER: 150 mw

TYPICAL SIGNAL CONDITIONER - SC 21

CIRCUIT:

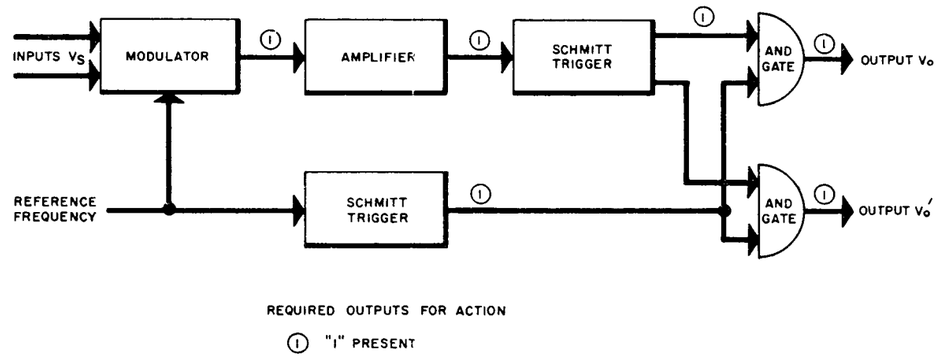


FIGURE E-9
TYPICAL SIGNAL CONDITIONER - SC 21

TYPICAL SIGNAL CONDITIONER - SC25

FUNCTION:	AC to DC Converter
INPUT:	AC Analog Voltage (V_i)
OUTPUT:	DC Voltage V_o
RELIABILITY:	$\lambda_f = 0.07 \times 10^{-4}$
	$\lambda_m = 0.22 \times 10^{-4}$
ACCURACY:	±2%
SIZE:	1.11 in^3
WEIGHT:	0.012 lb
POWER:	50 mw

READI FORM NO. 2

TYPICAL SIGNAL CONDITIONER- SC25

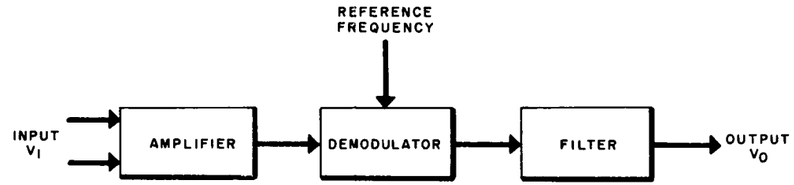


FIGURE E-10
TYPICAL SIGNAL CONDITIONER-SC25

- External commands
- Decision blanking
- Component self-check logic.

The function and source of these external commands are discussed in Appendix D, and the decision blanking and component self-check logic are discussed later in this appendix.

Upon conducting the decisions to the engine controls, the checkout-hold gates route signals to the parameter references and decision blanking. A discussion of the decision blanking appears in the next paragraph.

The parameter reference signals are used to change the threshold levels for malfunction detection in the continuous malfunction detection channels and selects the proper stored constants for signal processing in the serial digital computer. A discussion of this function appears in Appendix J.

G. DECISION BLANKING

The function of the decision blanking circuits is to initiate the control signals used to erase, delay or inhibit the malfunction indicators and potential decisions. The blanking command signals are initiated under the following conditions.

1. Time-to-go

The time-to-go to stage burn-out determines the mission value of some potential decisions. Should a malfunction occur close to the stage burn-out time, the implementation of the resulting decision may not yield any value to the mission and could actually result in a mission loss because of alterations in the flight profile. Decisions of this type are, therefore, inhibited as a function of time-to-go.

2. Decision Priority

The priority of decisions resulting from two or more engine malfunctions is determined by the decision blanking circuits. The decision to shut down an engine, for example, takes priority over the previous decision to increase the thrust in that engine.

3. Engine Response to Decisions

The initiation of a decision such as increasing of thrust results in engine transients and requires changes of the comparator threshold levels. During the engine response time, malfunction indicators and the resulting decisions could be generated due to these transients. To eliminate erroneous decisions sensed during these transient responses, the detection of certain malfunctions is inhibited until the engine attains its final operating values. In addition to this inhibiting of erroneous decisions, certain malfunction indicators result in decisions which require the sequential operation of the engine controls, such as an attempt to restart an engine after shut-down. The decision blanking circuit, therefore, contains the decision delay circuits required to sequence the engine controls.

H. SELF-CHECK

The ability to check a component or circuit for proper operation with a self-contained checkout system is called self-check. The object of the self-check circuits in READI is to reduce the false alarm rates resulting from failures in the less reliable components. The two failure modes which are sensed are failed high and failed low.

- Failed high is the failure of a component or circuit in READI in such a direction as to give a high output signal.
- Failed low is the failure of a component or circuit in READI in such a direction as to give a low output signal.

The two areas where the component or circuit unreliability warrants the use of self-check are the transducers and the serial digital computer.

1. Transducer Self-Check

The value of READI is reduced because of the high false alarm rate (10×10^{-4} typical) associated with transducers. By detecting the failure of a transducer which results in a false alarm, the value of READI is increased significantly. There are three methods of failure detection discussed in Appendix B which are considered feasible. They are:

- Sensor impedance self-check
- Reasonableness self-check
- Rate of change self-check

a. Sensor Impedance Self-Check

Catastrophic failure of the electrical element of a transducer results in either a short circuit or open circuit appearing across the element. By sensing the increase or decrease in current in the transducer element circuit caused by this open or short circuit, a failure of the transducer is detected.

The technique implemented to indicate a transducer failure by sensing the abnormal current flow depends upon the type of transducer to be checked. Figure E-11 illustrates two techniques which are used when the required output is proportional data, i.e., dual coil pressure transducer. The amplitude of the input to the self-check circuit is used to sense whether the transducer electrical element is opened or shorted. The self-check circuit compares the input voltage to one of the possible thresholds, failed high or failed low, depending upon which one indicates a false alarm. The sensed transducer failure information is then used in the component self-check logic to inhibit potential decisions resulting from this false alarm.

The data output signal of some transducers is a state signal (valve position transducer) that senses which of two positions the variable has attained. Since the amplitude accuracy of the signal from this two state device is not critical, a transformer or separate winding on the transducer coil may be used to sense an abnormal current without affecting the data output. Either an open circuit or short circuit in the electrical element of the transducer will result in a zero output; therefore, only one threshold is required to indicate a false alarm or missed alarm independent of the failure mode.

A typical transducer, using sensor impedance self-check, would have a false alarm rate of 5×10^{-4}.

b. Reasonableness Self-Check

Failure of a transducer, either electrically or mechanically, will cause the data output of the transducer to attain values which are outside of the predicted minimum or maximum output limits. The sensing of a transducer failure by the use of these limit conditions is called reasonableness self-check. The value of the limit conditions is specified in two ways.

(1) Transducer Limited Outputs

Many transducers have a minimum and maximum output which is determined by some electrical or mechanical limitation within the transducer, i. e. , mechanical stops of the strain gauge pressure transducer. By selecting output values outside of these predicted values, an upper and lower limit is established for the normal output. If the transducer output is detected exceeding this upper limit or falling below this lower limit, a signal is generated and fed to the component self-check logic indicating that the transducer has failed. The selection of the failure direction to be indicated is determined by the direction which results in a false alarm.

(2) Parameter Limited Outputs

The parameter which the transducer is measuring has a normal operating range under all conditions from which predictable minimum and maximum values may be obtained,as illustrated in figure E-12. By detecting when the transducer output is above or below the upper or lower limits, which is selected outside of the maximum and minimum predicted outputs, a failure in the transducer is detected. The particular limit chosen for the failure indication is determined by the false alarm mode. This detected false alarm is then used in the component self-check logic to inhibit any potential decisions triggered by the false alarm.

The reasonableness check is performed by the computer in the proposed READI system. The stored parameter limits are subtracted from the measured parameter value, the sign of the result determines the measured data's reasonableness. The check is controlled by the program memory and may be altered to meet any new requirements. The strain gauge pressure transducers and the resistance thermometers reasonableness checks are performed in the computer for the proposed READI system. The false alarm rates for a typical transducer are reduced to 0.1×10^{-4}, by use of reasonableness self-check.

c. Rate of Change Self-Check

Some parameters, either due to the inertia of the engine or the characteristic of the malfunction to be detected, cannot change value instantaneously but have some finite slope as a function of time. The output of transducer measuring parameters of this type, figure E-13 provides an efficient means of detecting either an electrical or mechanical failure in the transducer. The rate of

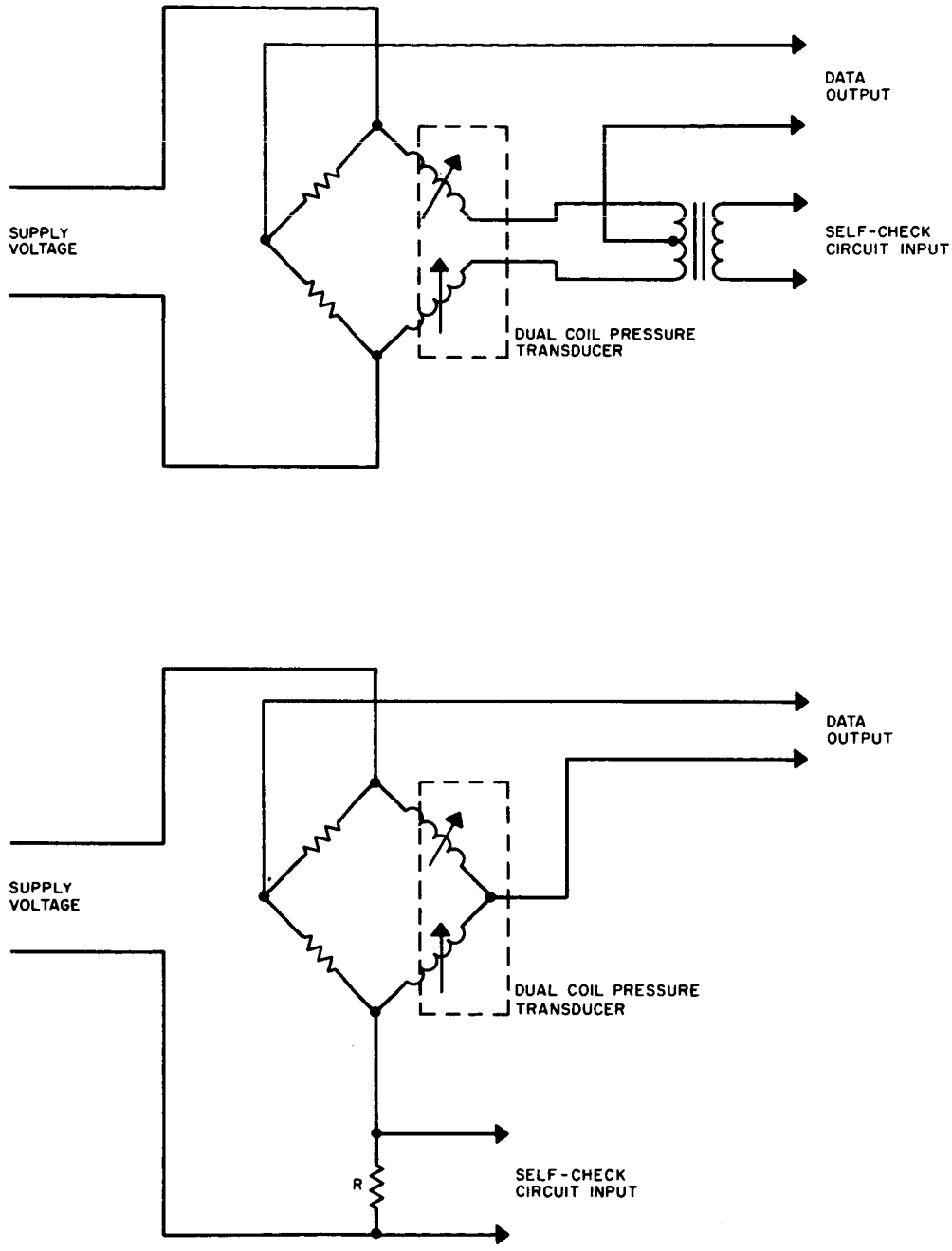


FIGURE E-11
SENSOR IMPEDANCE SELF-CHECK

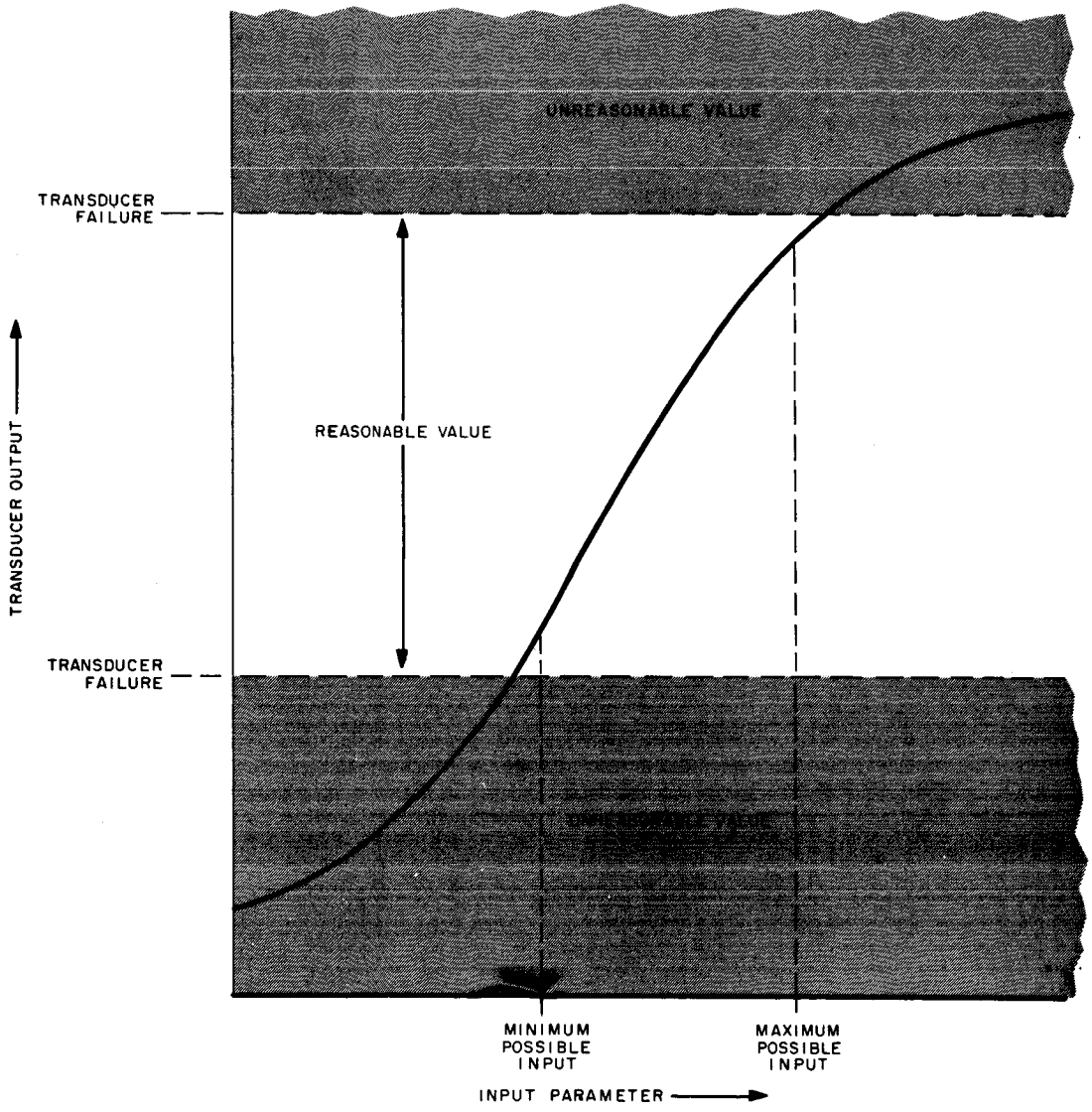


FIGURE E-12

RESONABLENESS SELF-CHECK
(LIMITED BY INPUT PARAMETER)

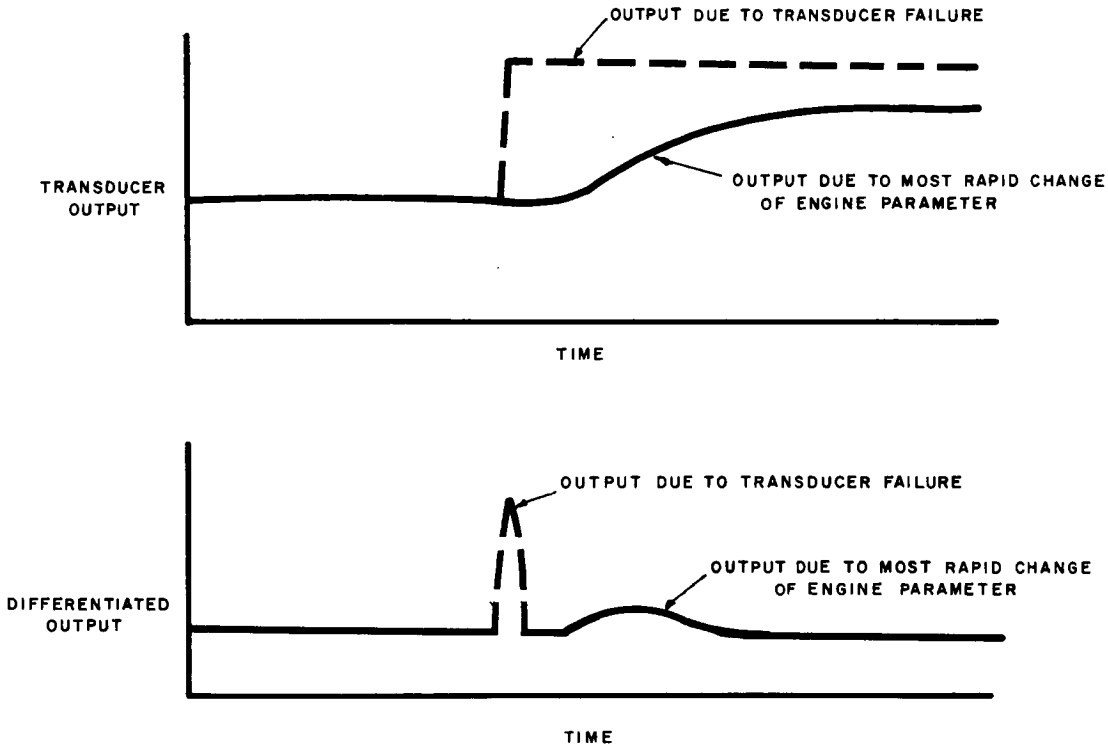


FIGURE E-13

RATE OF CHANGE SELF-CHECK

change of the transducer output is faster when a sensor failure occurs than the rate of change predicted for the parameter; therefore, the output may be differentiated and the fast rise time of the output used to detect the failure of the transducer. The direction of failure of the transducer to be sensed by the self-check circuit is determined by the direction of failure resulting in false alarms. A circuit of this type is used in sensing fire detector false alarms due to shorted elements. The false alarm rates of transducers are decreased by a factor of 100 when this method is used.

2. Serial Digital Computer Self-Check and Parity Check

The serial digital computer consists of the input interface circuits (multiplexer and analog-to-digital converter), arithmetic unit, program and data memory, and control circuits. The false alarm rate for this computer (2×10^{-4}) is considered too high for the proposed READI system; therefore, self-check is implemented to reduce the false alarm rate to 0.05×10^{-4}.

The computer is self-checked by introducing a known input voltage into the analog-to-digital converter which encodes this known stimuli into binary form for the arithmetic unit. This binary word is then processed by the arithmetic unit and compared to the correct value which is stored in the computer memory. Should the computed answer differ from the stored value, the computer will transfer a failure signal to the component self-check logic to inhibit the potential decision triggered by the failure. The sequence of operations required to self-check the computer is stored in the wired-program memory of the computer and is initiated when a potential decision results which involves the computer. This self-check method will indicate the proper or improper operation of the analog-to-digital converter and the arithmetic and control units and gate or inhibit the potential decisions accordingly.

The program and data memory words are checked whenever implemented by the computer by the use of odd parity check. Odd parity check is accomplished by adding a bit space to the required word length and inserting or deleting a pulse in this added bit space to generate an odd-numbered bit word in storage. A single error in the word will result in an even bit word which will be sensed as a word error. Error signals from the parity check circuits are implemented in the component self-check logic to eliminate incorrect decisions resulting from word errors.

3. Component Self-Check (Selection/Test Logic)

The component self-check logic provides the signals which gate the decision outputs to the engine controls upon receipt of self-check and parity check signals, indicating proper component and circuit operation. The following signals are implemented in determining the proper operation of the components and circuits utilized in the processing of a decision:

D(N) - the potential decision

V_m - the malfunction indicators used in arriving at decision D(N).

CH_n - the output of the self-check circuits of the transducers used in detecting V_m.

C_c - the computer self-check circuit output

C_p - the output of the parity check circuits in the computer.

Assuming that the READI system has indicated a potential decision (D(N)) due to the generation of the proper malfunction indicators (V_m), the self-check matrix will enable this decision when the following conditions are met:

- All the transducer self-check outputs CH_n indicate that the transducers associated with this decision have not failed in the false alarm mode.
- Parity check (C_p) of the stored and encoded binary words indicates that all words are correct.
- The computer self-check output (C_c) indicates that the serial digital computer is operating properly.

If the parity check output indicates an erroneous work, the potential decision and malfunction indicators are disabled and erased from storage. Should the associated transducers indicate a false alarm or the computer be operating improperly, the potential decision and malfunction indicators are disabled, erased from storage, and the generation of additional decisions which use the failed transducer or computer is inhibited.

The self-check logic could be implemented by the use of micrologic or magnetic logic. For this proposed READI system, micrologic was selected for the self-check logic because of its simplicity and reliability.

E-3. COMPONENT DESCRIPTION

A. TRANSDUCERS

The considerations in the selection of transducers for the READI system are covered in Appendix B. For each signal to be measured a trade-off is effected among the following factors:

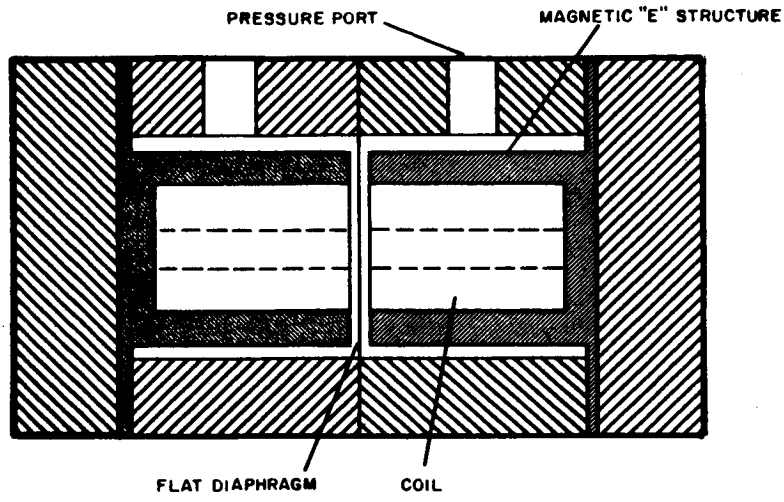
- reliability
- accuracy
- form of output
- availability
- weight
- cost.

A preliminary selection of sensor types for a second stage READI design is given in table E-2. The estimated "failed high" and "failed low" reliability data is the result of a survey of transducers currently used in rocket engine testing.

Typical of the simpler type of transducer recommended for READI is the flat diaphragm, variable reluctance-pressure sensor. As an example, this sensor is evaluated for each of the six criteria listed above.

1. Reliability

Compared to all other pressure sensor types, the variable reluctance sensor is among the very simplest. Consider the cross-section sketch below. The unit consists of a symmetrical arrangement of the "E" type inductance coils and a flat pressure diaphragm.



Mechanically, it is even simpler than most strain gauge sensors, since no structure is required to hold the strain gauge elements. The failure modes of the unit are:

mechanical - diaphragm rupture or deformation

- leakage

electrical - shorts and opens in the coils

2. Accuracy

The variable reluctance unit described here is suitable only for moderate accuracy requirements in the ±5 percent range. This accuracy reflects all of the errors in the sensor, i.e., temperature, hysteresis, linearity, etc.

3. Form of Output

Typical units have a coil inductance in the 30 to 500 millihenry range. When subjected to 100 percent pressure, one coil increases about 10 percent in inductance and the other decreases 10 percent. The output voltage is large enough such that no amplification is required for most of the associated parallel signal conditioning circuits. A potentiometer type sensor could provide an even larger voltage output but is ruled out because of complexity. For those pressure signals which are encoded and applied to the digital arithmetic computer, the d-c output of the strain gauge type is preferred.

4. Availability

Variable reluctance pressure sensors are readily available in a variety of pressure and inductance ranges. Special designs can be made for cases where, for instance, a large over-pressure must be accommodated. The latter is done by arranging the pole pieces of the coil to support the diaphragm so as to reduce the stress during overpressure transients.

5. Weight

The installed weight of the variable reluctance sensor is estimated to be 0.8 pound, most of which is due to the installation. Typical strain gauge units weigh about 1.4 pounds installed. The installation weight includes tubing, brackets, connectors and four feet of electrical cable. With a cost-weight trade-off factor of $100 per pound in the second stage, differences in this range; i.e., 0.6 pound, are negligible.

6. Cost

The cost of the variable reluctance type pressure sensors is in the $300 range, assuming special handling of standard units is required. Similar strain gauge units cost about $200 more. Depending on the system cost-risk trade-off, this difference in cost may be significant, especially if a large number of sensors is involved.

Similar trade-off evaluations were made on the other sensors in the system. The final selection of sensors for a READI system will be strongly influenced by the results of transducer investigations presently being conducted at the major rocket engine manufacturers. These investigations are aimed at finding suitable transducers for telemetry. The plan is to have the engine delivered with transducers installed and wired to a control engine junction box. A similar installation scheme has been recommended for READI system transducers.

TABLE E-2

TRANSDUCER CHARACTERISTICS

Code No.	Parameter	Description of Sensor	Estimated Failure Rate per Mission X 10^4 Failed High	Failed Low	Estimated Installed Weight (lb)
0	Elec. Input	No sensor	0	0	0
1	Flow	Turbine type flow-meter with temperature and pressure trim corrections to obtain mass flow.	8	20	4
2	Pressure Variable reluctance	Two coil, flat diaphragm variable reluctance pressure sensor for low to medium accuracy requirements; strain gauge pressure sensors for high accuracy requirements.	2	8	0.8
2	Pressure, strain gauge		4	16	1.4
3	Speed	Magnetic pulse pickup; tabs or slots in rotating member produce pulse rate proportional to speed.	0.1	1	0.6

TABLE E-2 (Cont)

TRANSDUCER CHARACTERISTICS

Code No.	Parameter	Description of Sensor	Estimated Failure Rate per Mission X 10^4 Failed High	Failed Low	Estimated Installed Weight (lb)
4	Fire	Continuous element variable resistance type fire sensor. Exposure of short length of element to fire causes an approximate resistance change from 10,000 ohms to 10 ohms.	20	20	1.5
5	Position	Single coil variable inductance; movement of valve causes magnetic core to be inserted or removed from coil. Single position indication only.	0.1	1	0.5
6	Temperature	Thermocouple (chromelalumal) for gas generator temperature, resistance element for propellant temperatures.	0.1	5	1.0

TABLE E-2 (Cont)

TRANSDUCER CHARACTERISTICS

Code No.	Parameter	Description of Sensor	Estimated Failure Rate per Mission X 10^4 Failed High	Failed Low	Estimated Installed Weight (lb)
7	Vibration	Velocity pickup-single coil, self-generating magnetic seismic pickup. (Crystal accelerometers are not used, because of their high impedance, susceptibility to damage and moisture and drift of calibration.)	0.1	3	0.6
8	Explosion (pressure)	Pressure sensor, variable reluctance, high threshold.	1	10	0.8

B. COMPUTER

1. Microelectronic Components

Except for the digital memory unit which consists of permalloy cores and bi-apperture ferrites, the use of microelectronic circuits for all computer functions was indicated in previous sections of this appendix. The superior reliability and lower cost realized with these solid-state circuits over the more conventional types are the principal factors dictating a microelectronic READI computer. These advantages will become particularly significant for electronic equipment design scheduled for 1964 production and beyond. Other advantages such as reduced weight, volume, and power are secondary considerations in the READI design.

Data-supported reliability documented by Fairchild on certain integrated semiconductor circuits already indicate failure rates as low as 0.046%/1000 hours. This is between 20 to 60 times better than that realized with single transistors (Mil-grade, non-Minuteman type). In making this comparison, it is to be noted that an integrated circuit, although composed of a single piece (chip) of silicon material, is equivalent to a complete electronic network with active and passive components. Perhaps more significant to the development of READI is the component reliability improvement being projected for microelectronics. Figure E-14 illustrates Texas Instrument's integrated circuit reliability projected through 1963, by which time failure rates of 0.001%/1000 hours or better are forecasted. The rapidly advancing microelectronic technology brought about by heavy Government and industrial investment lends considerable credance to this forecast.

Costs of commercially available, integrated semiconductor circuits are being sharply reduced; 1961 prices of these devices have been reduced by two of the leading suppliers from a $120 to $450 range to a $20 to $50 range. Small quantity unit prices of $5 to $15 are projected for digital integrated circuits in 1963.

An example of one manufacturer's line of digital integrated circuits currently available is illustrated in figure E-15. This is Fairchild's family of six compatible building blocks termed "Micrologic", suitable combinations of which are sufficient to satisfy all the digital logic functions of the READI computer. These circuits are among other manufacturers' circuits which have been tested and qualified by Sperry for operation at a 1-mc clock rate operating over a -55°C to +125°C ambient temperature. Exclusive use is made of direct coupled transistor logic which is the simplest means of implementing digital logic. Fairchild assembles each "Micrologic" block into industry standard (JEDEC) TO-5, TO-18, or TO-47 eight lead packages. The most common microcircuit package marketed today is the TO-5 which is shown in figure E-16.

Reference has been made thus far only to the integrated semiconductor network type of microcomponent. There are, in fact, a diverse number of microcircuit components being developed and manufactured. Thin film, multichip, and other microcircuit techniques will also be required in READI to implement the more specialized linear and analog circuits such as demodulators, voltage amplifiers, power amplifiers, passive filters, and oscillators. The state-of-the-art development of single-chip, integrated semiconductor networks for such analog applications is inadequate to warrant their consideration at this time.

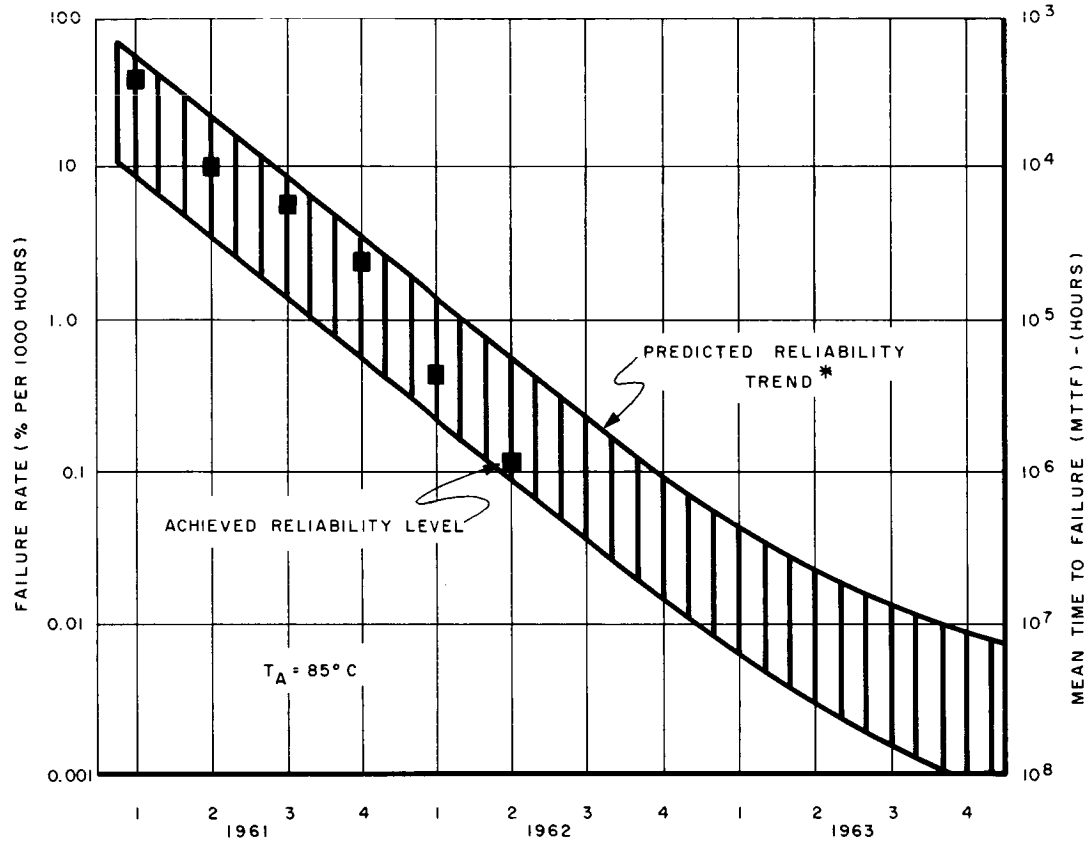
2. Packaging Concepts

The need for ultra-reliable performance transcends all other considerations in the packaging design to be adopted for the READI computer. In microelectronic equipment design, the major failure mechanism and principal problem experienced by the packaging engineer is interconnections. The problem is two-fold. First, difficulties are realized in making interconnections between modules; and second, is the complication which results in connecting multi-lead microcircuit devices, the leads of which project into a very limited area of a printed circuit board.

The layout design of a basic module is an important phase in the physical design of microelectronic equipment. The proper design of a basic module will permit reduction of large, complex electronic systems to smaller repetitive subassemblies. One packaging philosophy which prevails in industry today is to design for maximum volumetric efficiency by making the module subassembly as expendable "throw-aways". Cost is a principle factor in this module design concept. However, interconnection between the modules must also be considered in terms of reliability requirements. The larger the module, the fewer the required interconnections in the system. The number of interconnections, in fact, tends to increase in proportion to the square of the number of modules. Thus, the final module size invariably reflects a trade-off between the reduction of system interconnections and the increased cost of microcircuit components contained in the expendable module.

The expendable module concept has considerable merit in those large quantity, military weapon system applications where maintainability is an important factor and reliability requirements are perhaps not as stringent as those established for READI. The READI system on the other hand is characteristically a "custom" designed, relatively small quantity NASA launch vehicle application. The modular packaging approach recommended for READI does not use the expendable module concept; it is based rather, on the following design criteria:

- Each module shall be repairable in that integrated circuit, thin film, or other microcircuit elements can be easily disassembled from the module. Consequently, throw-away cost is not a factor. This applies to in-plant and field maintenance; launch site repair will be on a complete unit replacement basis.



* DATA BASED ON A SEMICONDUCTOR NETWORK THAT PERFORMS THE SAME ELECTRICAL FUNCTION AS APPROXIMATELY 20 EQUIVALENT DISCRETE COMPONENTS CONNECTED AS A CIRCUIT.

FIGURE E-14

INTEGRATED SEMICONDUCTOR NETWORK RELIABILITY TREND AND PREDICTIONS

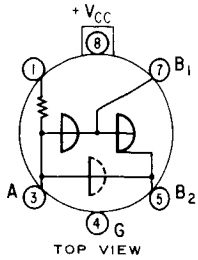
PRELIMINARY CHARACTERISTICS

MICROLOGIC ELEMENT "B"

BUFFER

SUPPLY VOLTAGE + 3 V_{dc} ± 30%
POWER DISSIPATION 25 mW (TYP)
TEMPERATURE -55°C TO +125°C

$B_1, B_2 = \bar{A}$



INPUT (TERMINAL 3) - CAN BE DRIVEN BY ANY MICROLOGIC ELEMENT - 2.2 MICROLOGIC LOADS

OUTPUT (TERMINAL 5) - CAN DRIVE UP TO 25 OTHER MICROLOGIC ELEMENT LOADS IN PARALLEL (TERMINAL 7) – CAN DRIVE UP TO 5 OTHER MICROLOGIC ELEMENT LOADS IN PARALLEL
(NOTE - TERMINALS 5 AND 7 MAY NOT BE USED CONCURRENTLY)

AVERAGE DELAY - (TERMINAL 5) -60 nsec., (TERMINAL 7) - 50 nsec.

MULTIVIBRATOR OPERATION - CONNECTING TERMINALS 1 AND 8 PROVIDES A POSITIVE RETURN FOR A CAPACITOR INPUT TO TERMINAL 3.

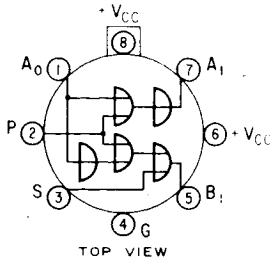
PRELIMINARY CHARACTERISTICS

MICROLOGIC ELEMENT "C"

COUNTER ADAPTER

SUPPLY VOLTAGE +3 V_{dc} ±30%
POWER DISSIPATION 75 mW (TYP.)
TEMPERATURE -55°C TO +125°C

$\bar{A}_1 = \bar{A}_0 \bar{P}$
$\bar{B}_1 = A_0 \bar{P} + S$



INPUT - CAN BE DRIVEN BY ANY MICROLOGIC ELEMENT.
A_0, P (TERMINALS 1, 2) - 2 MICROLOGIC LOADS
S (TERMINAL 3) - 1 MICROLOGIC LOAD.

OUTPUT (TERMINALS 5, 7) - CAN DRIVE UP TO 5 OTHER MICROLOGIC ELEMENT LOADS IN PARALLEL.

AVERAGE DELAY - 100 nsec.

NOTE - THE NODE RESISTORS OF THE OUTPUT INVERTERS ARE RETURNED TO TERMINAL 6 WHICH IS NORMALLY CONNECTED TO THE SUPPLY VOLTAGE.

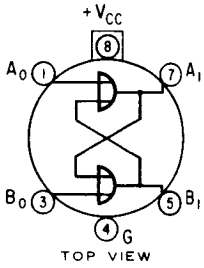
PRELIMINARY CHARACTERISTICS

MICROLOGIC ELEMENT "F"

FLIP - FLOP

SUPPLY VOLTAGE + 3 V_{dc} ± 30%
POWER DISSIPATION 30 mW (TYP.)
TEMPERATURE -55°C TO +125°C

$\bar{A}_1 = B_1 + A_0$
$\bar{B}_1 = A_1 + B_0$



INPUT (TERMINALS 1, 3) - CAN BE DRIVEN BY ANY MICROLOGIC ELEMENT - 1 MICROLOGIC LOAD.

OUTPUT (TERMINALS 5, 7) - CAN DRIVE UP TO 4 OTHER MICROLOGIC ELEMENT LOADS IN PARALLEL.

AVERAGE DELAY - 50 nsec.

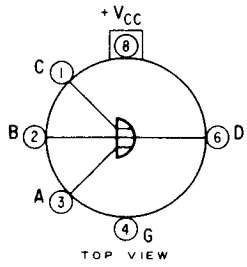
PRELIMINARY CHARACTERISTICS

MICROLOGIC ELEMENT "G"

GATE

SUPPLY VOLTAGE + 3 V_{dc} ± 30%
POWER DISSIPATION 15 mW (TYP.)
TEMPERATURE -55°C TO +125°C

$D = (\overline{A + B + C})$



INPUT (TERMINALS 1, 2, 3) - CAN BE DRIVEN BY ANY MICROLOGIC ELEMENT - 1 MICROLOGIC LOAD.

OUTPUT (TERMINAL 6) - CAN DRIVE UP TO 5 OTHER MICROLOGIC ELEMENT LOADS IN PARALLEL.

AVERAGE DELAY - 50 nsec.

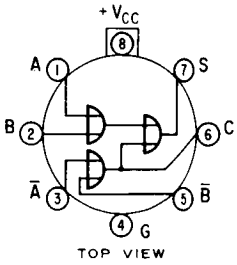
PRELIMINARY CHARACTERISTICS

MICROLOGIC ELEMENT "H"

HALF ADDER

SUPPLY VOLTAGE + 3 V_{dc} ± 30%
POWER DISSIPATION 45 mW (TYP.)
TEMPERATURE -55°C TO +125°C

$S = A\bar{B} + \bar{A}B$
$C = AB$



INPUT (TERMINALS 1, 2, 3, 5) - CAN BE DRIVEN BY ANY MICROLOGIC ELEMENT - 1 MICROLOGIC LOAD.

OUTPUT (TERMINAL 6) - CAN DRIVE UP TO 4 OTHER MICROLOGIC ELEMENT LOADS IN PARALLEL.

OUTPUT (TERMINAL 7) - CAN DRIVE UP TO 5 OTHER MICROLOGIC ELEMENT LOADS IN PARALLEL.

AVERAGE DELAY - (TERMINAL 6) - 50 nsec., (TERMINAL 7) - 100 nsec.

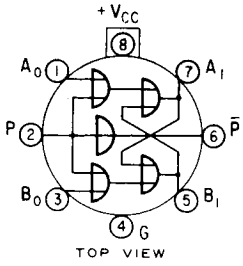
PRELIMINARY CHARACTERISTICS

MICROLOGIC ELEMENT "S"

HALF SHIFT REGISTER

SUPPLY VOLTAGE + 3 V_{dc} ± 30%
POWER DISSIPATION 75 mW (TYP.)
TEMPERATURE -55°C TO +125°C

$\bar{A}_1 = B_1 + \bar{A}_0 \bar{P}$
$\bar{B}_1 = A_1 + \bar{B}_0 \bar{P}$



INPUT - CAN BE DRIVEN BY ANY MICROLOGIC ELEMENT.
A_0, B_0 (TERMINALS 1, 3) - 1 MICROLOGIC LOAD.
P (TERMINAL 2) - 3 MICROLOGIC LOADS.

OUTPUT (TERMINALS 5, 7) - CAN DRIVE UP TO 4 OTHER MICROLOGIC ELEMENT LOADS IN PARALLEL.
(TERMINAL 6) - CAN DRIVE 5 OTHER MICROLOGIC LOADS.

AVERAGE DELAY - 100 nsec.

FIGURE E-15

FAIRCHILD "MICROLOGIC" INTEGRATED CIRCUITS

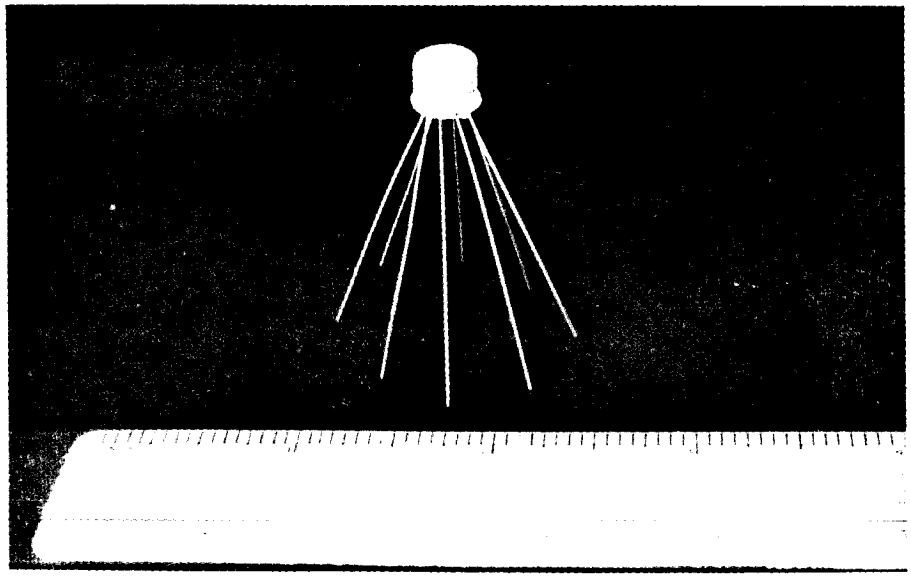


FIGURE E-16

TYPICAL INTEGRATED CIRCUIT PACKAGE; TEDEC TO-5 SIZE

- Modules will be limited to a thickness of only one electronic part. No attempt will be made to achieve high packaging density at the expense of interconnection reliability, fabrication ease, serviceability and cooling.
- Module size will be as large as practical, consistent with rigidity requirements, so as to minimize interconnections between modules.

The module geometry most compatible with these criteria and consequently recommended for READI is the flat plate substrate. The multi-layer printed conductor techniques recently devised make the substrate well suited for micromodule assembly. The microcircuit components are suitably bonded and electrically connected to the substrate. All external connections would be made at one edge of the board. Adequate spacing would be provided between the elements on a substrate and between the substrates themselves so that the soldering of connections is simplified and potential hotspots minimized.

The substrate geometry is close to ideal in minimizing the number of external, flexible wire connections. In addition it affords an effective means for virtually eliminating the need for plug-in type connectors in the computer. Sperry's experience has shown that connectors are a major failure item in electronic equipment. To eliminate the need for module connectors, a book-type assembly of flat substrates is recommended in which hand-soldered wiring connections are made between the common board edges. By unfolding the boards, access to all parts for repair and servicing is provided. A penalty is incurred in this reliable assembly technique, however, in that to remove a substrate, every wire must be disconnected by hand-soldering.

A special consideration in the packaging design is to simplify the programming of decision rule logic for different launch vehicles and missions. One method which appears quite feasible is to provide a multi-layer printed wired patchboard which would interconnect the decision rule modules.

3. Environmental Design Characteristics

There are three main hostile environments to be considered in the physical design of the computer. They are:

a. Shock and Vibration

The isolation design approach recommended is to:

- provide a strong, relatively large mass case for the computer and mount the unit directly to the stage structure. The objective in this isolation technique is to attenuate the higher frequency components of vibration conducted by the structure and engine chamber sounds.
- provide a resilient suspension of the electronic chassis to the case. This isolation is designed to attenuate a band of lower frequency components above some frequency to be determined. Under normal engine operating conditions, the need for this isolation design is questionable. It is recommended, however, as added assurance of satisfactory computer operation in view of the severe shock and vibration environment, particularly during an engine malfunction.

b. Ambient Pressure

The electrical arcing, electronic component bursting, lack of convection cooling, and other dangers associated with a near vacuum pressure environment necessitates the assembly of the computer chassis within a pressurized inert gas container. A cylindrically shaped container is recommended because of the relative ease with which it can be hermetically sealed.

c. Temperature

Indications are that the temperature environment will not be a major READI design problem. Some heating of the computer may be necessary prior to engine firing because of the relatively close proximity of the computer to the cryogenic propellant tanks. This could best be achieved by means of a heating jacket around the cylindrical case of the computer. During the latter phases of stage flight the temperature of the installation compartment will increase. The prospects are that the engine heat shield will be effective in limiting the temperature to an acceptable range. Temperature increases within the computer case will also be limited by thermal lags, especially that due to the computer case, and the relatively short stage burning times. If future estimates indicate that the temperatures will exceed 125°C, additional thermal shielding will be provided for the computer. Most computer circuits will operate satisfactorily over a temperature range of -55°C to +125°C. The temperature for the A-D converter, however, must be within a 100°C band if the accuracy of this unit is to be maintained.

Appendix F

READI EVALUATION SCHEME

Appendix F

APPENDIX F

READI EVALUATION SCHEME

F-1. INTRODUCTION

An evaluation scheme for a given READI system applied to a given vehicle and mission complex has been developed and implemented on a scientific type general purpose digital computer. The purpose of this scheme is to compare, on a numerical basis, the effectiveness of various READI systems and to vary the vehicle and/or the mission with a fixed READI system. The latter procedure produces information on the sensitivity of READI system design to assumptions about the vehicle and/or the mission complex.

System merit is described in two dimensions by its effectiveness in reducing risk and by the cost of obtaining this function.

In general, a risk is defined as a sum of terms of the form $L_j P(j)$, where L_j is the loss incurred by the occurrence of the event j and $P(j)$ is the probability of the occurrence of the event j. The units of loss are normalized to the replacement value of mission results.

A perfect READI system for a given vehicle and mission complex is defined as an ideal READI system which monitors all known malfunction areas and never makes any incorrect decisions (including the decision to take no action). Elements in the risk increment with respect to this reference result from the following factors:

- A particular system will not monitor all known malfunction areas.
- A physically realizable system may not indicate some decision (other than no action) when the condition of the engine is such that the decision should be indicated. These events are referred to as missed alarms.
- A physically realizable system may indicate some decision (other than no action) when no action should be taken. These events are referred to as false alarms.

- A physically realizable system may indicate some decision (other than no action) when, indeed, some other decision (other than no action) should be indicated. These events are referred to as wrong alarms.

In addition to cost and risk, it is also desirable to define a system acceptability criteria for manned missions based on the minimum acceptable probability of crew survival. In the present analysis this factor is taken into consideration in the characterization of the mission.

F-2. DEVELOPMENT AND SIMPLIFICATION OF THE INCREMENTAL RISK EXPRESSION

Let ΔR be the incremental risk with reference to the perfect system for a fixed READI system. Then, following the discussion in paragraph F-1, expressions shown in table F-1 are obtained. (Symbols are defined in table F-3.) The convention is established that $d_{k_o,\ p} = d_{o,\ p}$ and that m_o indicate no engine malfunction.

Several simplifications to ΔR may now be made. First of all, the terms in the risk decrement due to wrong alarms are all either zero or quite small. This is the case since

$$P(d_{k_j,\ p} = 1/m_j)\ P(m_i,\ p)$$

is small when $i \neq j$. When

$$i = j,\ L_p(d_{k_j,\ p};\ m_i) - L_p(d_{k_i,\ p};\ m_i) = 0.$$

Therefore, the risk decrement due to wrong alarms will be neglected.

The second simplification results from the fact that

$$L_p(d_{o,\ p};\ m_o) = 0$$

for all p. Thus in the expression for the risk reference we may drop away the five $i = o$ terms. Also

$$L_p(d_{o,\ p};\ m_o) - L_p(d_{k_o,\ p};\ m_i = o) = 0$$

TABLE F-1

BASIS OF INCREMENTAL RISK EXPRESSION

Source	Algebraic Expression
Risk Reference (Perfect System)	$\sum_{p=1}^{5} \sum_{i=0}^{I} L_p(d_{k_i}, p; m_i)\, P(m_i, p)$ (1)
Risk Decrement Due to not Monitoring all Malfunction Areas (Transducer Perfect system)	$\sum_{p=1}^{5} \sum_{i=0}^{I} (1-S_{i,p}) [L_p(d_o, p; m_i) - L_p(d_{k_i}, p; m_i)] \cdot P(m_i, p)$ (2)
Risk Decrement Due to Missed Alarms	$\sum_{p=1}^{5} \sum_{i=0}^{I} S_{i,p} [L_p(d_o, p; m_i) - L_p(d_{k_i}, p; m_i)] \cdot P(d_{o,p} = 1/m_i)\, P(m_i, p)$ (3)
Risk Decrement Due to False Alarms	$\sum_{p=1}^{5} \sum_{k=1}^{ks} [L_p(d_k, p; m_o) - L_p(d_o, p; m_o)] \cdot P(d_{k,p} = 1/m_o)\, P(m_o, p)$ (4)
Risk Decrement Due to Wrong Alarms	$\sum_{p=1}^{5} \sum_{i=1}^{I} \sum_{j=1}^{ks} [L_p(d_{k_j}, p; m_i) - L_p(d_{k_i}, p; m_i)] \cdot P(d_{k_j,p} = 1/m_i)\, P(m_i, p)$ (5)
Incremental Risk	$\Delta R = (1) + [(2) + (3) + (4) + (5)]$

L_p loss in phase, p

d decision rule

m malfunction

$S_{i,p}$ I if m_i monitored in phase p

P probability

Subscripts

p phase index

k decision index

i malfunction index

o indicates no action or no malfunction

Thus in the perfect transducer system expression and the missed alarm expression we may also drop away the five i = 0 terms.

The final simplification of ΔR has to do with replacing the quantity $P(d_{o,p} = 1/m_i)$ with another quantity which is simpler to compute. To accomplish this simplification, we introduce an intermediate Boolean variable, I_i, called the malfunction indicator for engine malfunction area m_i. The purpose of this intermediate variable is twofold. First, it enables us to expand decision rules, which are general Boolean functions of the signal space separations, as Boolean sums of the I_i's in a manner such that each term on the sum may be associated with the occurrence of a particular m_i. The generation of the I_i expansion of two decision rules is illustrated in figure F-1. It will be noted that in the expansion of d_2 in figure F-1 the term V_4 is repeated. Thus the I_i expansion of a decision rule does not represent its simplest Boolean form. Also, it will be noted that, in general, the I_i's are general Boolean functions of the signal space separations. The second reason for introducing the I_i's is that one may now assume that if m_i occurs and is programmed to lead to a unique decision, then READI indicates its presence by setting $I_i = 1$ only. Thus,

$$P(d_{o,p} = 1/m_i) = P(I_i = 0/m_i)$$

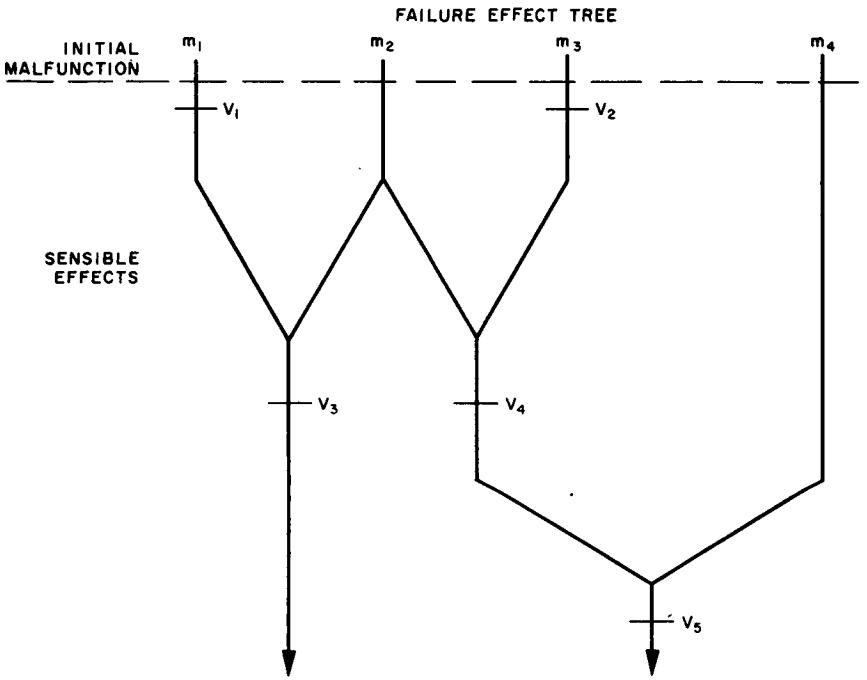
It should be emphasized that the introduction of the I_i's is for the purpose of simplifying computations only, and does not represent the basic design philosophy of the system.

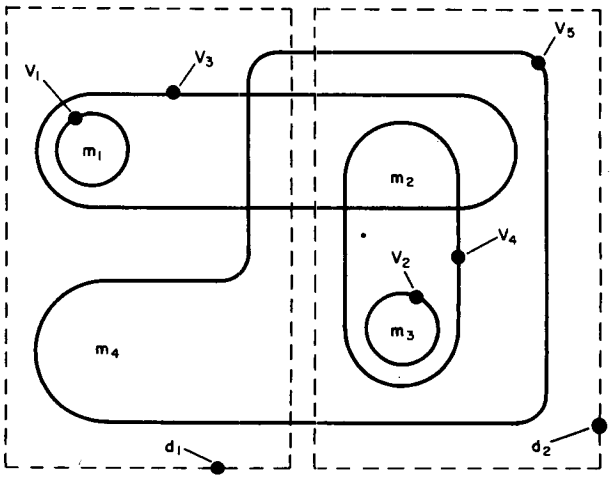
Thus, making use of all the previous assumptions and simplifications, one may obtain the expressions for each component of ΔR as shown in table F-2.

A digital computer program has been written to evaluate each summation in ΔR and to evaluate ΔR. This program is presently divided into two main sections. The first section evaluates the loss data required by

$$\Delta R, \text{ i.e., } L_p(d_{k_i,p}; m_i);\ L_p(d_{o,p}; m_i) \text{ and } L_p(d_{k',p}; m_o).$$

The second section takes this loose data, combines it with a system and engine description, and computes the summations on a ΔR and system cost.





m, d, V, LOGIC DIAGRAM

FIGURE F-1
EXPANSION OF DECISION RULES

LOGICAL EQUATIONS:

$$d_1 = V_1 + V_5\bar{V}_4 + V_3\bar{V}_4 + V_3\bar{V}_5 = (V_1 + V_3\bar{V}_4 + V_3\bar{V}_5) + V_5\bar{V}_4 = I_1 + I_4$$

$$\text{WHERE} \begin{cases} I_1 = V_1 + V_3\bar{V}_4 + V_3\bar{V}_5 \\ I_4 = V_5\bar{V}_4 \end{cases}$$

$$d_2 = V_2 + V_4 + V_3\bar{V}_1 = (V_2 + V_4) + (V_4 + V_3\bar{V}_1) = I_2 + I_3$$

$$\text{WHERE} \begin{cases} I_2 = V_4 + V_3\bar{V}_1 \\ I_3 = V_2 + V_4 \end{cases}$$

SYMBOLS:

m_i MALFUNCTION

$I_i(V)$ MALFUNCTION INDICATION - (SET OF V TERMS USED IN A DECISION RULE THAT INDICATES A GIVEN MALFUNCTION)

V_j SIGNAL SPACE SEPARATION - (DEFINED BY THE SET OF m_i CONTAINED IN THE V)

d_k DECISION

TABLE F-2

FINAL FORM OF INCREMENTAL RISK EXPRESSION

Source	Algebraic Expression
Risk Reference (Perfect System)	$\sum_{p=1}^{5} \sum_{i=1}^{I} L_p(d_{k_i}, p; m_i) P(m_i, p)$ (1)
Risk Decrement Due To Not Monitoring All Malfunction Areas (Transducer Perfect System)	$\sum_{p=1}^{5} \sum_{i=1}^{I} (1-S_{i,p}) [L_p(d_o, p; m_i) - L_p(d_{k_i}, p; m_i)] \cdot P(m_i, p)$ (2)
Risk Decrement Due To Missed Alarms	$\sum_{p=1}^{5} \sum_{i=1}^{I} S_{i,p} [L_p(d_o, p; m_i) - L_p(d_{k_i}, p; m_i)] \cdot P_p(I_i = 0/m_i) P(m_i, p)$ (3)
Risk Decrement Due To False Alarms	$\sum_{p=1}^{5} \sum_{k=1}^{ks} L_p(d_{k,p}; m_o) P(d_{k,p} = 1/m_o) P(m_o, p)$ (4)
Risk Decrement Due To Wrong Alarms	Assumed Negligible
Incremental Risk	$\Delta R = (1) + [(2) + (3) + (4)]$

TABLE F-3

SYMBOLS

Symbol	Definition
p	Engine phase index numbers, p = 1, ---, 5.
i	Malfunction area index number.
k	Decision rule index number.
$d_{k,p}$	Decision k in engine phase p.
$d_{o,p}$	"No action" decision in engine phase p.
$d_{k_i,p}$	The programmed decision for malfunction area i in engine phase p.
m_i	Malfunction area i.
m_o	No malfunction.
$Lp(d_{k_i,p}; m_i)$	The loss incurred when m_i occurs in engine phase p and the programmed decision is made.
$Lp(d_{o,p}; m_i)$	The loss incurred when m_i occurs in engine phase p and the no action decision is made.
$P(m_{i,p})$	The probability of malfunction area i in engine phase p.
$P(d_{o,p} = 1/m_i)$	The conditional probability that in engine phase p of "no action" given m_i has occurred.
$P(d_{k,p} = 1/m_o)$	The conditional probability that in engine phase p decision k is made given no malfunction has occured.
$P(d_{k_j,p} = 1/m_i)$	The conditional probability that in engine phase p decision k_j is made given malfunction i has occured.
ΔR	Incremental risk.
I	Maximum value of i for the propulsion system under consideration.
K_s	The maximum value of K for the READI system under consideration.
I_i	The malfunction indicator for m_i.
$P_p(I_i = O/m_i)$	The probability that in engine phase p that I_i = O given that m_i occurs.
$S_{i,p}$	One if m_i is monitored in engine phase p, zero otherwise.

F-3. EVALUATION OF INCREMENTAL RISK COMPONENTS

A. BASIC APPROACH TO THE PROBLEM

The main problem in the evaluation of the summations involved in ΔR is the evaluation of the quantities $P(I_i = 0/m_i)$ and $P(d_{k,p} = 1/m_o)$. Several techniques employing combinatorial analysis and probability theory were investigated and found to be satisfactory from a theoretical point of view. However, it was found that if these evaluation techniques were employed, it would be difficult to make the entire system description input to the computer. Considering the volume of the planned evaluation computations, it was decided to employ an alternate approach to these computations.

This alternate approach to the evaluation of $P(I_i = 0/m_i)$ and $P(d_{k,p} = 1/m_o)$ is essentially a sensor malfunction tracer routine. Its basic ideas are as follows. Assume first that a given engine malfunction area has occurred. Second, assume that all sensors but one are in their normal conditions for the assumed malfunction area occurring and that this sensor is failed in a known mode. Determine if the event under consideration (i.e. $I_i = 0$ or $d_{k,p} = 1$) occurs. If so, add the probability of the failed sensor, being in the particular failed mode, to the probability being computed. When this is done for all sensors and all failure modes within each sensor, the resulting sum is taken as the conditional probability of the event under consideration.

It will be assumed that each sensor has only two failure modes: high and low.

The validity of the sensor malfunction tracer routine for computing the above conditional probabilities rests, in the main, on the following two assumptions in addition to those made in paragraph F-2. First, two or more sensors are never in a failed condition at any given instant during the operation of READI. Since the probability that two sensors fail during a given launch operation is quite small, the effects of the violation and this assumption are at least second order and may be neglected. Second, the high and low failure modes of a given sensor are of sufficient amplitude so that they dominate the indication of any signal space separation in which that sensor occurs. The significance of this assumption may be seen by considering a simple example. Suppose signal space separation V_j is derived from a single sensor output S_L, and that the definition of binary one for V_j takes the form

$$V_j = \begin{cases} 1 \text{ if } S_L > x \\ 0 \text{ if } S_L \leq x \end{cases}$$

where x is some real number. Then if S_L fails high, $V_j = 1$ and if S_L fails low, $V_j = 0$, independent of the value of x. The existence of self-check provisions, such as reasonableness checks built into the READI data processing circuitry, may well vitiate this assumption. The existence of such checks will be neglected here. Additional analyses, based on additional and presently unavailable information, are required to access the effects of self-check provisions on sensor outputs.

B. DETAILS OF THE $P(I_i = 0/m_i)$ COMPUTATION

Consider a fixed engine phase. If I_i is not contained in any of the Boolean sums making up the decision rules (other than no action), then it will not be necessary to compute $P(I_i = 0/m_i)$ in that decision rule, since the term $S_{i,p}$ will be zero. If, however, it does occur in one such decision rule, we shall compute its value. As stated, I_i is a Boolean function of some signal space separations. It is assumed that the following forms may occur:

$$V_{K_1}$$
$$V_{K_1} V_{K_2}$$
$$V_{K_1} + V_{K_2}$$
$$V_{K_1} V_{K_2} + V_{K_3}$$
$$V_{K_1} V_{K_2} + V_{K_3} V_{K_4}$$

where V_K is a particular signal space separation. If a complemented V occurs we replace it by a new V with a different subscript. Given the form of each I_i and the values of each V_K occurring in that I_i when a particular sensor fails in each of its two failure modes, and the other sensors have their normal values for m_k occurring, it is a simple matter to determine the value of I_i. If for a particular sensor failed in a particular mode, it is found that $I_i = 0$, the probability of that sensor failing in that mode is added to $P(I_i = 0/m_i)$. This is done for each sensor in each failure mode and the resulting cumulative sum is $P(I_i = 0/m_i)$ under the above assumptions.

A flow diagram for the computer routine to carry out the computation is shown in figure F-2. The form of each I_i; the values of each V in I_i for each sensor in each failure mode, assuming the other sensor have their normal values for m_i occurring; the form of all decision rules occurring in each engine phase; and the probabilities of sensor failure high and low are taken as inputs to this program.

C. DETAILS OF THE $P(d_{k,p} = 1/m_o)$ COMPUTATION (FALSE ALARM)

The procedure for this computation is essentially the same as those for $P(I_i = 0/m_i)$. The exact procedure for this computation may be best understood by considering a simple example. Let

$$d_{k,p} = I_{i_1} + I_{i_2} + I_{i_3}$$

for some fixed values of k and p. Assume that sensor L = 1 has failed high and that all other sensors have their normal output for no engine malfunction. Determine whether I_{i1} is zero or one under these conditions. If it is one, add the probability of sensor L = 1 failing high to $P(d_{k,p} = 1/m_o)$ and consider L failed low and all other sensors in their normal conditions for no engine malfunction. Thus, in this case we do not proceed to examine the remaining I_i. The reason for this is that the Boolean function

$$1 + I_{i_2} + I_{i_3}$$

is one independent of the values of I_{i2} and I_{i3}. Therefore, if under the above conditions I_{i2} is also one, it would not be correct to add the sensor failure probability to $P(d_{k,p} = 1/m_o)$ twice. If, however, $I_{i1} = 0$, then we proceed to consider I_{i2} with sensor L = 1 failed high, and the above procedure is repeated, and I_{i3} is considered if necessary. This procedure is then repeated for all other sensors and the resulting cumulative sum is $P(d_{k,p}/m_o)$ for the fixed values of k and p chosen, under the above assumptions.

Examination of the form of ΔR shows that it is necessary to set $P(d_{k,p}/m_o)$ to zero if decision k does not occur in engine phase p.

A flow diagram for the computer routine to perform this computation is shown in figure F-3. Inputs to this routine are the specification of the form of each $d_{k,p}$ specification of the form of each I_i in terms of its V's and their Boolean combination, the value of each V when sensor L is failed high or low and all other sensors have their normal output for no engine malfunction, and the low and high sensor failure probabilities.

D. ADDITIONAL COMPUTATIONS

The computation of ΔR and its components now directly follows given values of the loss factors. This is discussed in paragraph F-6. Additional information required is the value of $P(m_{i,p})$ for $i \geq 1$, the values of I, K_S, and $S_{i,p}$ for all $i \geq 1$ and $p = 1, ---, 5$. We need note that

$$P(m_{o,p}) = 1 - \sum_{i=1}^{I} P(m_{i,p})$$

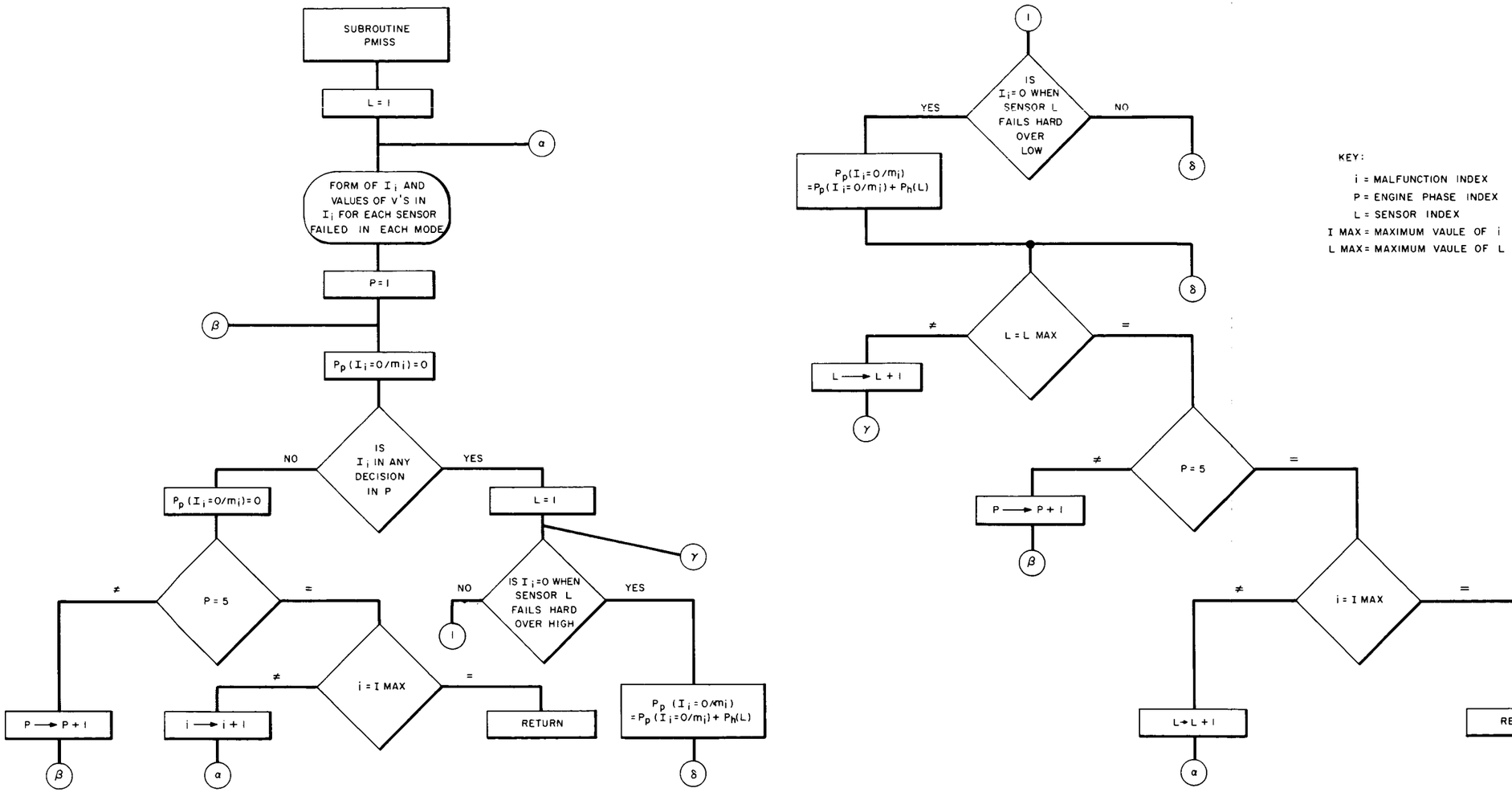
where $P(m_{i,p}) = 0$, if malfunction index number i does not occur. These computations are performed in subroutine SRISK of the computer program in a straightforward manner.

F-4. COMPUTATION OF SYSTEM COST

The elements of system cost considered are:

- Transducer cost
- Weight penalty converted to dollars
- Installation cost
- Signal conversion costs
- Development costs amortized over 20 vehicles
- Fixed system cost.

A development cost of 6 million dollars in the period 1964 to 1966 was assumed, of which 12 percent is attributed to sensors. A fixed system cost of $200,000 and a weight penalty of $100 per pound suitable to the second stage of a three stage vehicle were assumed. All systems costs were then distributed over the sensors in proportion to the complexity of signal conversion for each, so that the total cost of all sensors was equal to the total system cost including all factors mentioned above.



KEY:

i = MALFUNCTION INDEX
P = ENGINE PHASE INDEX
L = SENSOR INDEX
I MAX = MAXIMUM VAULE OF i
L MAX = MAXIMUM VAULE OF L

FIGURE F-2
COMPUTER FLOW DIAGRAM SUBROUTINE P MISS

Thus, in order to compute the system cost, we need only have a list of the adjusted cost of all sensors, calculated as above, and a list of the actual sensors used in the system under study. The computation of system cost is carried out in subroutine SCOST of the computer program in a straightforward manner as the sum of the adjust costs of the sensors used in the system.

F-5. COMPUTER PROGRAM

An overall flow diagram for the computer program is shown in figure F-4.

F-6. EVALUATION OF LOSS FACTORS

The quantitative penalties incurred by the set of joint events $(d_{k,\,p};\ m_i)$ must be known in order to evaluate a READI system in the manner discussed in a previous paragraph. The evaluation is specifically for the second stage of a three stage launch vehicle. Thus, only those events $(d_{k,\,p};\ m_i)$ occurring in the second stage performance interval are considered.

The following assumptions are made in defining the set $(d_{k,\ p};\ m_i)_{\ t}$ existing in stage 2 at a time t:

- The index i assumes only one value other than "0", i. e., the joint probability of any two malfunctions is vanishingly small.
- The index k assumes only one value other than "0", i. e., the joint probability of any two decisions is approximately zero.

The first assumption is borne out by typical rocket engine statistics. The second is valid for a properly designed READI system. Thus, we may examine each $(d_{k,\ p};\ m_i)$ condition individually and obtain its corresponding $L_p\,(d_{k,\ p};\ m_i)$ independently.

Briefly the analysis proceeds in the following way:

A joint event $(d_{k,\ p};\ m_i)$ influence upon the mission status can best be studied by noting its effect upon the rocket stage terminal velocity. A particular ΔV, or velocity decrement, can be assigned to each event $(d_{k,\ p};\ m_i)$.

Initially $(d_{k,\ p};\ m_i)$ affects the following parameters: specific impulse, propellant mass flow rate, and propellant-on-board. The decrements in these values are translatable through the rocket engine equation into a ΔV.

The magnitude of a particular ΔV incurred by a $(d_{k,\ p};\ m_i)$ will place the stage in one of three levels of operational performance defined as follows in table F-4.

TABLE F-4

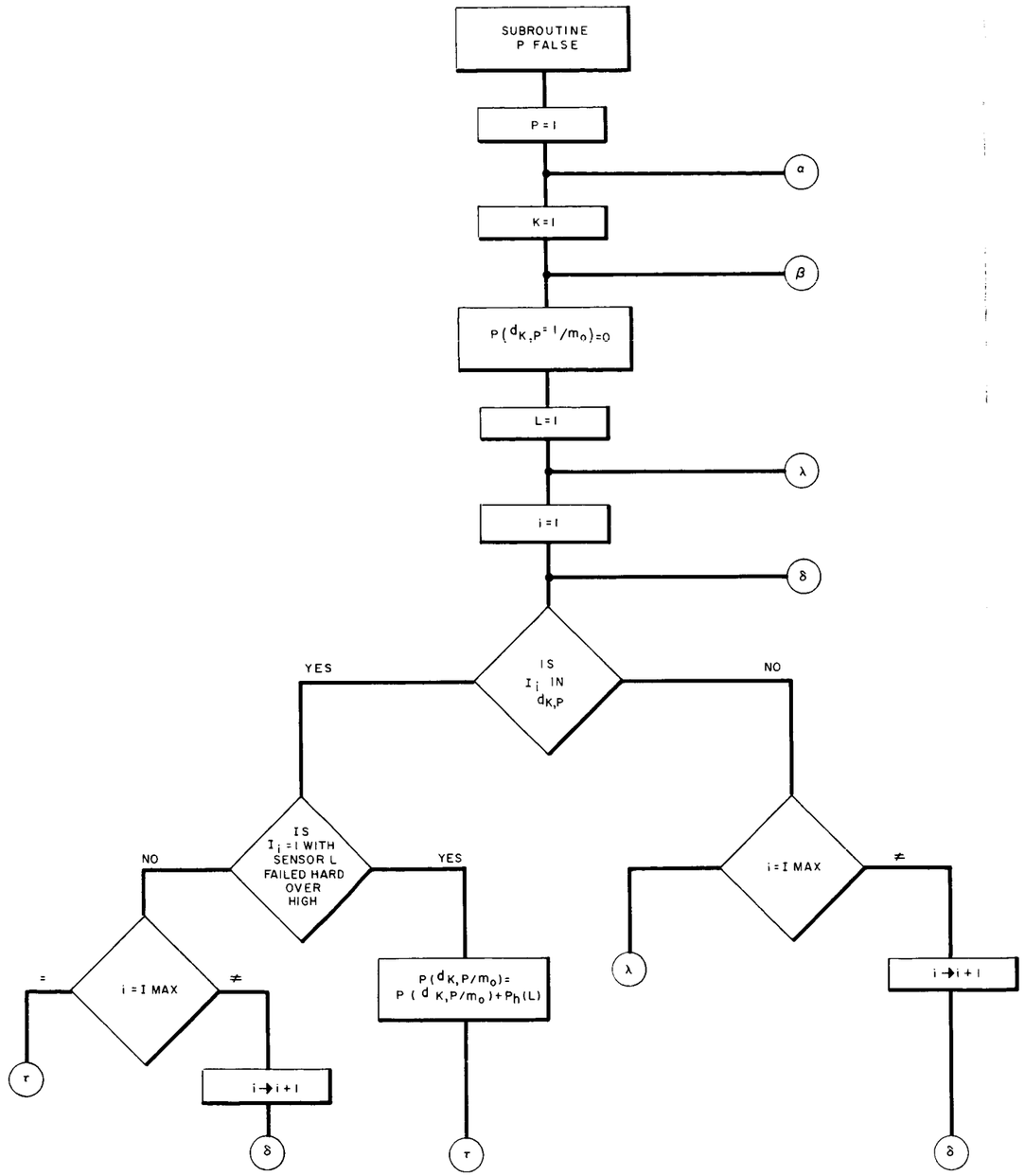
OPERATIONAL PERFORMANCE CATEGORIES

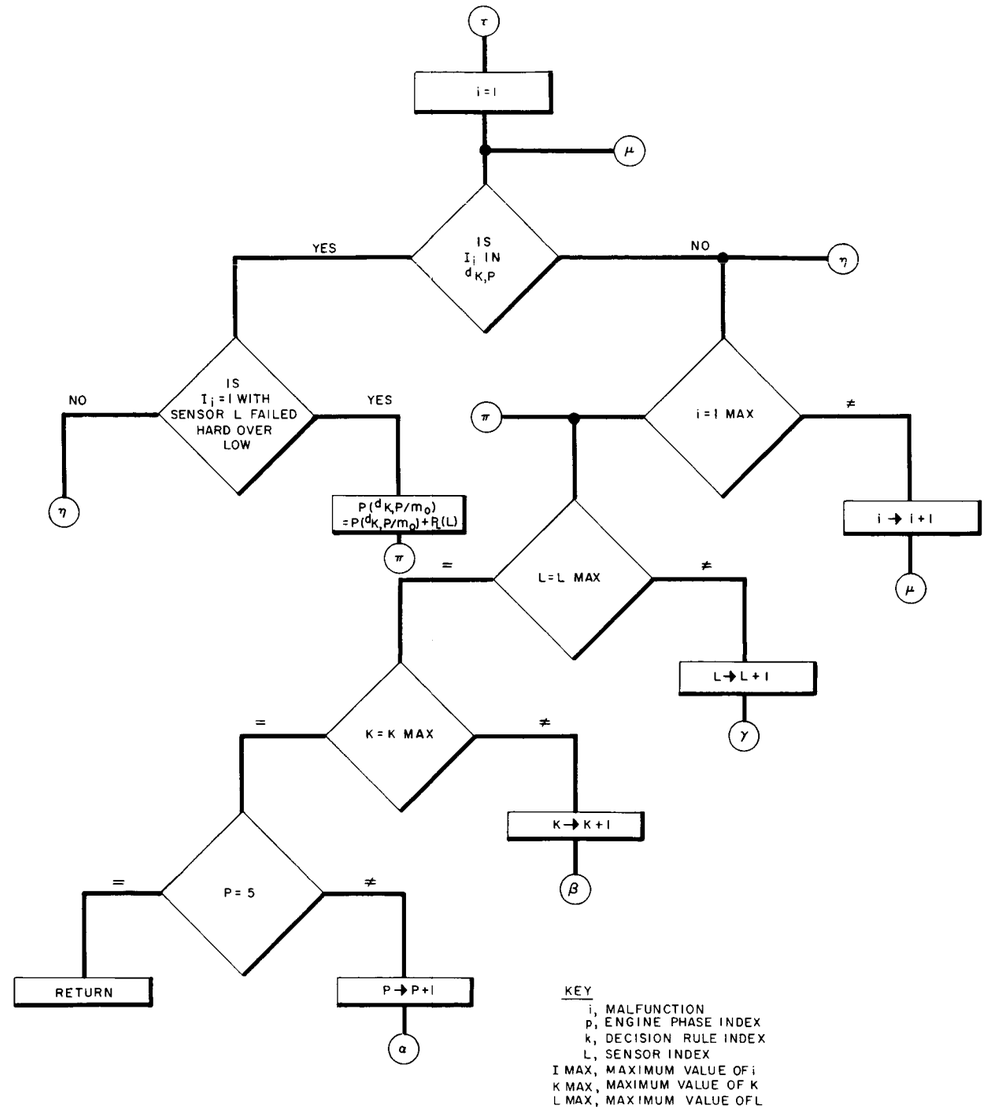
Operational Performance Level or Category	Description
Failed	Propulsion subsystem unsatisfactory
Degraded	Propulsion subsystem performance marginal. Vehicle can attain mission objective only if following stages operate perfectly.
Normal	Propulsion subsystem performance satisfactory. Vehicle will attain mission objective, barring failure of the following stage.

Additional to these three operational categories is the category of "exploded". The probability of event $(d_{k,\ p};\ m_i)$ mapping into this category is determined by statistical study of typical rocket engines. It is noted here that these categories are mutually exclusive, and the sum of their probabilities of occurrence, conditional on the event $(d_{k,\ p};\ m_i)$, is unity. The probabilities of the attainment of these operational categories for a particular $(d_{k,\ p};\ m_i)$ are used in a matrix analysis of the entire vehicle-mission complex.

This analysis generates an assigned loss value for the particular $(d_{k,\ p};\ m_i)$ event under analysis.

Thus a set $[L_p(d_{k,\ p};\ m_i)]$ is generated with a one-to-one correspondence to a set of events $[(d_{k,\ p};\ m_i)]$.





KEY
- i, MALFUNCTION
- p, ENGINE PHASE INDEX
- k, DECISION RULE INDEX
- L, SENSOR INDEX
- I MAX, MAXIMUM VALUE OF i
- K MAX, MAXIMUM VALUE OF K
- L MAX, MAXIMUM VALUE OF L

FIGURE F-3
COMPUTER FLOW DIAGRAM SUBROUTINE P FALSE

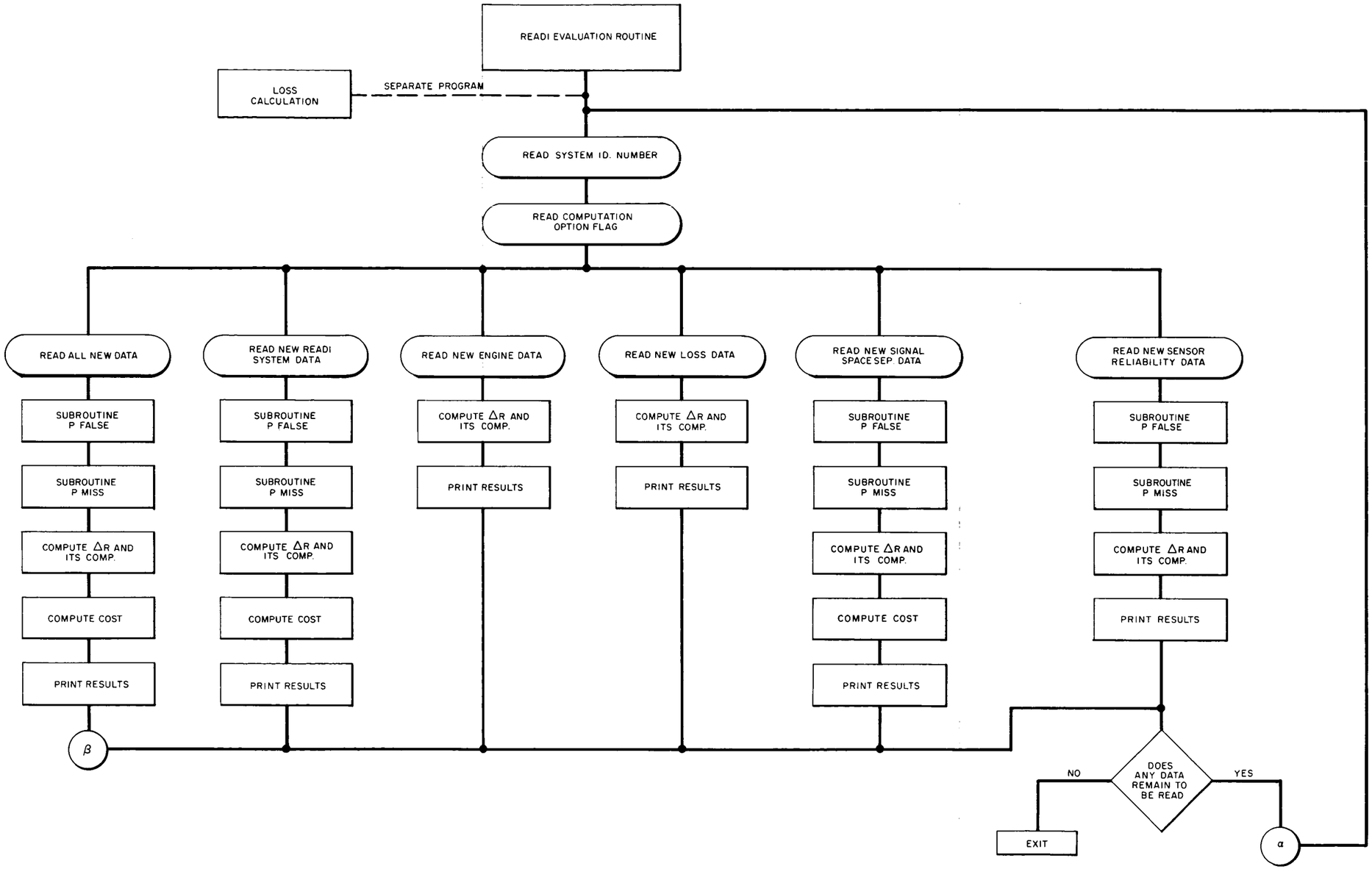


FIGURE F-4
MAIN COMPUTER FLOW DIAGRAM EVALUATION ROUTINE

It is interesting to note that with the restrictions assumed in defining a particular set $[(d_{k,\ p};\ m_i)_t]$, the values $[L_p(d_{k,\ p};\ m_i)]$ are independent of the size of $[(d_{k,\ p};\ m_i)]$. This enables us to compute a single set of loss data and apply it to a large number of READI systems.

A. VEHICLE MISSION COMPLEX

It is necessary first to define the vehicle-mission complex as a framework into which the stage operational category analysis can be inserted. Figure 3-3 illustrates the mission, indicating the transitions between mission states.

Specifically the end states are defined as follows:

I - Successful prime mission (crew survives)

II - Successful alternate mission (crew survives)

III - Mission lost, crew survives

IV - Mission lost, crew lost.

The end of boost states are defined as:

$(S3)_1$ = probability of successful boost to prime mission

$(S3)_2$ = probability of successful boost to alternate mission

$(S3)_3$ = probability of aborted mission

$(S3)_4$ = probability of explosion.

Additionally:

$(S1)_5$ = probability of 1st stage abort

$(S2)_4$ = probability of 2nd stage abort.

Further probabilities are specified as follows:

S_{10} = probability of successful prime mission after a successful boost to the prime mission

S_{20} = probability of successful alternate mission after a successful boost to the alternate mission

L_{10} = probability of crew loss, successful boost to prime mission

r_1 = probability of crew loss, first stage abort

r_2 = probability of crew loss, second stage abort

r_3 = probability of crew loss, third stage abort.

From the diagram, transformation matrices may be constructed allowing for calculation of the end-of-boost state probabilities.

$$\text{Thus, } (S3)_{J1} = (S1)_M \, T_{M,\,N} \, T_{N,\,J1} = (S2)_N \, T_{N,\,J1}$$

where

$(S3)_{J1}$ = state J1, end stage 3 (end of boost)

$(S3)_N$ = state N, end stage 2

$(S1)_M$ = state M, end of stage 1

$T_{M,\,N}$ = transistion matrix, end stage 1 to end stage 2

$T_{N,\,J1}$ = transistion matrix, end stage 2 to end stage 3 (end of boost)

From the parameters specified above we may compute the probability of altering each of the end states listed previously. For example,

$$P(I) = (S3)_1 \, S_{10}$$

$$P(II) = (S3)_2 \, S_{20}$$

$$P(III) = (1 - (S3)_1 S_{10} - (S3)_2 S_{20})$$

$$P(IV) = (S3)_1 L_{10} + (S3)_2 L_{20} + r_1 (S1)_5 + r_2 (S2)_4 + r_3 (S3)_3 + (S3)_4$$

where

$$(S3)_1 = (S1)_M T_{M,N} T_{N,1} = (S2)_N T_{N,1}$$

$$(S3)_2 = (S1)_M T_{M,N} T_{N,2} = (S2)_N T_{N,2}$$

$$(S3)_3 = (S1)_M T_{M,N} T_{N,3} = (S2)_N T_{N,3}$$

$$(S3)_4 = (S1)_M T_{M,N} T_{N,4} = (S2)_N T_{N,4}$$

$$(S2)_4 = (S1)_M T_{M,4}$$

Thus, $(S1)_M$, $T_{M,N}$, $T_{N,J1}$ and probability set A completely determine the probability of attainment of each of the end states.

As previously stated, the analysis is made here for the second vehicle stage. A similar analysis has been made for a first and third stage, assuming a typical READI system in each. From this preliminary analysis, values of $(S1)_M$ and $T_{N,J1}$ are generated.

Values for the probability set A are determined from general post-boost mission considerations.

The T-matrix, $T_{M,N}$, evolves from the stage operational category analysis.

B. STAGE OPERATIONAL CATEGORY ANALYSIS: DETERMINATION OF $T_{M,N}$ FOR PARTICULAR EVENT $(d_{k,p}; m_i)$

As mentioned previously, a particular joint event $(d_{k,p}; m_i)$ may be paired with a particular velocity decrement, ΔV, through its direct effect upon the parameters of specific impulse, propellant mass flow rate, and propellant-on-board.

Through the rocket engine equation the following relationship may be generated:

$$\Delta V = gI_{SP}\left[\frac{\ln (m_o/m)}{N}\left[\frac{\Delta I_{SP}}{I_{SP}}\right] + \frac{\Delta m}{m}\right]$$

where

ΔV = rocket velocity decrement

$\frac{\Delta I_{SP}}{I_{SP}}$ = functional loss in specific impulse, single engine

$\frac{\Delta m}{m}$ = fractional loss in mass.

$\Delta m/m$ is dependent upon four factors: the stage propellant margin, stage burning time margin, propellant mass flow rate (thrust), and a possible loss of propellant overboard. Specifically

$$\frac{\Delta m}{m} = \left[\frac{\Delta m}{m}\right]_{LOSS} - \left[\frac{\Delta m}{m}\right]_{MAX}$$ if all propellant is expended

or

$$= \frac{m_o - m}{m}\left[\frac{\Delta W}{W}\left[1 + \left[\frac{\Delta T}{T}\right]_{MAX}\right] - \left[\frac{\Delta T}{T}\right]_{MAX} + \left[\frac{\Delta m}{m}\right]_{LOSS}\right]$$

if all time is expended.

where

$\left[\frac{\Delta m}{m}\right]_{LOSS}$ = fractional loss in overboard propellant

$\frac{\Delta W}{W}$ = fractional loss in propellant mass flow rate, stage.

$\left[\frac{\Delta m}{m}\right]_{MAX}$ = propellant margin

$\left[\frac{\Delta T}{T}\right]_{MAX}$ = time margin

With a value of ΔV obtained for an event $(d_{k,p}; m_i)$, the operational category level placement due to this ΔV is determined. The seriousness of the velocity error is dependent upon the velocity correction capability of the offending and subsequent stages, and also the allowable end of boost, or final velocity error. The correction capabilities of the stages are depending in turn, upon

$$\left[\frac{\Delta m}{m}\right]_{MAX} \quad \text{and} \quad \left[\frac{\Delta T}{T}\right]_{MAX}$$ whichever is limiting. The

allowable end of boost velocity error, V_{END} is determined by the precision demanded by the mission.

Thus, stage velocity limits may be calculated which define, mathematically, the operational categories of "normal", "degraded", and "failed":

$$\Delta V_F = V_{END} + (V_{MAX})_3$$

$$\Delta V_o = 0.5\,(V_{END} + (V_{MAX})_3 - V^*)$$

where

$$(V_{MAX})_i = \min\left[(V_{MAX})_{T,\,i}; (V_{MAX})_{m,\,i}\right]$$

$$(V_{MAX})_{m,\,i} = \left[gI_{SP}\left[\frac{\Delta m}{m}\right]_{MAX}\right]_i$$

$$(V_{MAX})_{T,\,i} = gI_{SP}\left[\left[\frac{m_o - m}{m}\right]\left[\frac{\Delta T}{T}\right]\right]_i$$

$$V^* = \min\left[V_F; (V_{MAX})_2\right]$$

Thus for each condition $(d_{k,\,p}; m_i)$ incurring

$$\frac{\Delta I_{SP}}{I_{SP}}, \frac{\Delta W}{W}, \left[\frac{\Delta m}{m}\right] \quad \text{LOSS}$$

TABLE F-5*

IF	STAGE IS
$\Delta V < \Delta V_D$	NORMAL
$\Delta V_D < \Delta V < \Delta V_F$	DEGRADED
$\Delta V_F < \Delta V$	FAILED

a particular velocity decrement may be associated with it which, when compared with mathematically defined limits, in turn associates the condition with a particular operational performance category.

The resultant stage operational category determines $T_{M,N}$ for $(d_{k,p}; m_i)$.

C. DETERMINATION OF VELOCITY DECREMENT EQUATION PARAMETERS

The engine loss inputs to the mission loss calculations are reduced to the following categories:

- loss of thrust
- loss of specific impulse
- loss of propellant overboard
- probability of explosion.

Table I-2 summarizes the above losses for one of the engine systems which was investigated to evaluate various engine alternate capabilities. The losses are listed for no READI, READI operating correctly and for READI false alarm.

The losses used in the evaluations were calculated and/or estimated using representative performance coefficients for variations, such as the variation of specific impulse with O/F, the variation of thrust with O/F, etc.

- - - - - - -

*Note: Table F-5 applies for all engine phases except operate. The operate phase is accommodated by assuming that the condition $(d_k, p; m_i)$ occurs at a randome time, and then computing the percentage of vehicles which will fail, degrade, or be unaffected by random occurrence of the event.

1. Loss of Thrust

This loss is usually the complete loss of thrust of one engine due to an engine failure or READI action. For malfunction areas involving low and high propellant flow, either fuel or ox, the malfunction was arbitrarily defined at 20 percent above or below the normal flow. The thrust was then calculated from the reduced propellant flow.

2. Loss of Specific Impulse

The specific impulse loss is generally zero. In the case of some degradation type failures, such as low fuel flow, a specific impulse variation does occur and was calculated from the assumed performance coefficients, i.e. $\partial I_{sp} / \partial o/F$.

3. Loss of Propellant Overboard

Overboard propellant losses were arbitrarily defined, for cases where leakage occurred, as 20 percent of the nominal engine flow. For the case where the main propellant valve fails open, the flow, under tank head pressure, was estimated at 30 percent of normal.

4. Probability of Explosion

The probability of explosion, given in a malfunction, was estimated for each case, based on rocket test experience and intuitive reasoning. The chief sources of explosion are the accumulation of propellants, either in the main thrust chamber, igniter chamber, or gas generator, and the subsequent ignition by the spark igniters. Another prime contributor to explosion is combustion instability, which if allowed to proceed was assumed to destroy the engine. In two instances a destructive overspeed of the turbopump occurs: this is assumed to lead to explosion in 10 percent of the cases.

D. ASSIGNMENT OF LOSS VALUES TO END STATES; DETERMINATION OF $L_p (d_{k,\ p}; m_i)$ VALUE

It has been established that a set $(T_{m,n})$ can be generated in a one-to-one correspondance with a set of events $(d_{k,\ p}; m_i)$. In turn, $T_{m,n}$ enables the determination of the end state probabilities as discussed previously. By weighting these end states, i.e., attaching a loss value to each end state, a value of $L_p (d_{k,\ p}; m_i)$ is generated for each event. For example,

$$L_p(d_{k,\,p};\, m_i) = P(I)\,B_1 + P(II)B_2 + P(III)B_3 + P(IV)B_4$$

where B_n is the loss value of state n.

The values B_n, for each end state, take the form of quantities normalized to the replacement value of the prime mission, which is assigned a value of unity.

The values of B_n chosen for this analysis are

$$B_1 = 0,\ B_2 = 0.8,\ B_3 = 1,\ B_4 = 11$$

Substituting in the expression determined for the P ( ) yields $L_p(d_{k,\,p};\, m_i) = B_p(1 - (S3),\ S_{10}) - B_a(S3)_2\, S_{20} +$

$$B_p(S3),\ L_{10} + (S3)_2\, L_{20} + (S3)_4 + (S2)_4\, r_2 +$$

$$(S3)_3\, r_3 + (S1)_5\, r_1$$

$L_p(d_{k,\,p};\, m_i)$ may be split into two losses defined as follows:

$L_{p_m}(d_{k,\,p};\, m_i)$ = mission loss

$$= S_p(1 - (S3)_1\, S_{10}) - B_a(S3)_2\, S_{20}$$

$L_{p_c}(d_{k,\,p};\, m_i)$ = crew loss

$$= L_p(\ ) - L_{p_m}(\ )$$

In terms of the B_n

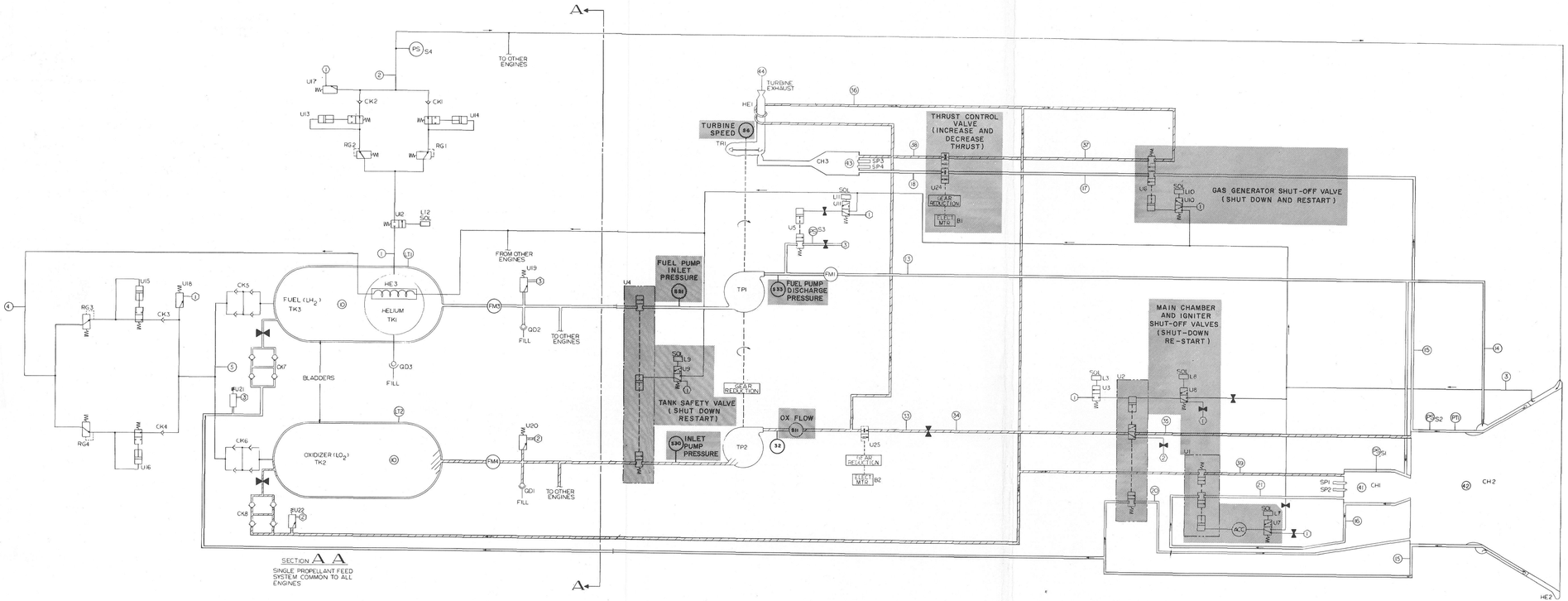
$$B_p = 1.0$$

$$B_a = 0.2$$

$$B_c = 1.0$$

Appendix G
READI MODEL ENGINE

Appendix G



LT2	OXIDIZER TANK LEVEL TRANSDUCER
LT1	FUEL TANK LEVEL TRANSDUCER
PT1	MAIN THRUST CHAMBER PRESSURE TRANSDUCER
SS1	TURBOPUMP SPEED SENSOR
SP3, SP4	GAS GENERATOR SPARK PLUG
SP1, SP2	IGNITER SPARK PLUG
GG1	TURBINE GAS GENERATOR
CH2	MAIN THRUST CHAMBER
CH1	MAIN THRUST CHAMBER IGNITER
FM4	OXIDIZER FLOW METER, TOTAL
FM3	FUEL FLOW METER, TOTAL
FM2	OXIDIZER FLOW METER, ENGINE
FM1	FUEL FLOW METER, ENGINE
TR1	TURBINE
TP2	OXIDIZER PUMP
TP1	FUEL PUMP
PS4	CONTROL GAS PRESSURE SWITCH
PS3	FUEL PUMP PRIME PRESSURE SWITCH
PS2	MAIN CHAMBER PRESSURE SWITCH
PS1	IGNITER CHAMBER PRESSURE SWITCH
QD3	HELIUM TANK QUICK DISCONNECT
QD2	FUEL TANK QUICK DISCONNECT
QD1	OXIDIZER TANK QUICK DISCONNECT
CK5-CK8	QUADRUPLE CHECK VALVE
CK1-CK4	CHECK VALVE
HE3	HELIUM TANK HEAT EXCHANGER
HE2	HELIUM HEAT EXCHANGER
HE1	OXIDIZER HEAT EXCHANGER
TK3	FUEL TANK
TK2	OXIDIZER TANK
TK1	HELIUM TANK
RG4	SECOND STAGE HELIUM PRESSURE REGULATOR
RG3	PILOTED STAGE HELIUM PRESSURE REGULATOR
RG2	FIRST STAGE HELIUM PRESSURE REGULATOR
RG1	FIRST STAGE HELIUM PRESSURE REGULATOR
EV	ELECTRIC MOTOR OXIDIZER CUT CONTROL VALVE
EV	ELECTRIC MOTOR TURBOPUMP CONTROL VALVE
U20	OXIDIZER SLY CONTROL VALVE ELECT MTR OPERATING
U24	TURBOPUMP CONTROL VALVE ELECT MTR OPERATING
U22	PRESSURIZATION RELIEF VALVE, OXIDIZER
U21	PRESSURIZATION RELIEF VALVE
U20	OXIDIZER RELIEF VALVE
U19	FUEL TANK RELIEF VALVE
U18	SECOND STAGE REGULATOR RELIEF VALVE
U17	FIRST STAGE REGULATOR RELIEF VALVE
U16	SECOND STAGE REGULATOR MALFUNCTION VALVE, PNEUMATIC OPERATING
U15	FIRST STAGE REGULATOR MALFUNCTION VALVE, PNEUMATIC OPERATING
U14	FIRST STAGE REGULATOR MALFUNCTION VALVE, PNEUMATIC OPERATING
U13	FIRST STAGE REGULATOR MALFUNCTION VALVE, PNEUMATIC OPERATING
U12	HELIUM PRESSURIZING VALVE, SOLENOID OPERATING
U11	FUEL PUMP PRIME VALVE, PILOT VALVE SOLENOID OPERATING
U10	TURBOPUMP SHUTOFF VALVE, PILOT VALVE SOLENOID OPERATING
U9	MAIN PROP VALVE, PILOT VALVE SOLENOID OPERATING
U8	MAIN PROP VALVE, PILOT VALVE, SOLENOID OPERATING
U7	IGNITER PROP VALVE, PILOT VALVE, SOLENOID OPERATING
U6	TURBOPUMP SHUTOFF VALVE, PNEUMATIC OPERATING
U5	FUEL PUMP PRIME VALVE, PNEUMATIC OPERATING
U4	FIRST SHUTDOWN VALVE, SOLENOID OPERATING
U3	FIRST SHUTDOWN VALVE, PNEUMATIC OPERATING
U2	MAIN PROP VALVE, PNEUMATIC OPERATING
U1	IGNITER PROP VALVE, PNEUMATIC OPERATING
DESIGNATION	DESCRIPTION

LEGEND
- (1) HELIUM OVERBOARD DRAIN
- (2) OXIDIZER OVERBOARD DRAIN
- (3) FUEL OVERBOARD DRAIN
- (ACC) ACCUMULATOR
- MECHANICAL LINK
- FIXED ORIFICE
- PRESSURE BUDGET STATION NO.

FIGURE G-1
READI MODEL ENGINE- FLUID SCHEMATIC

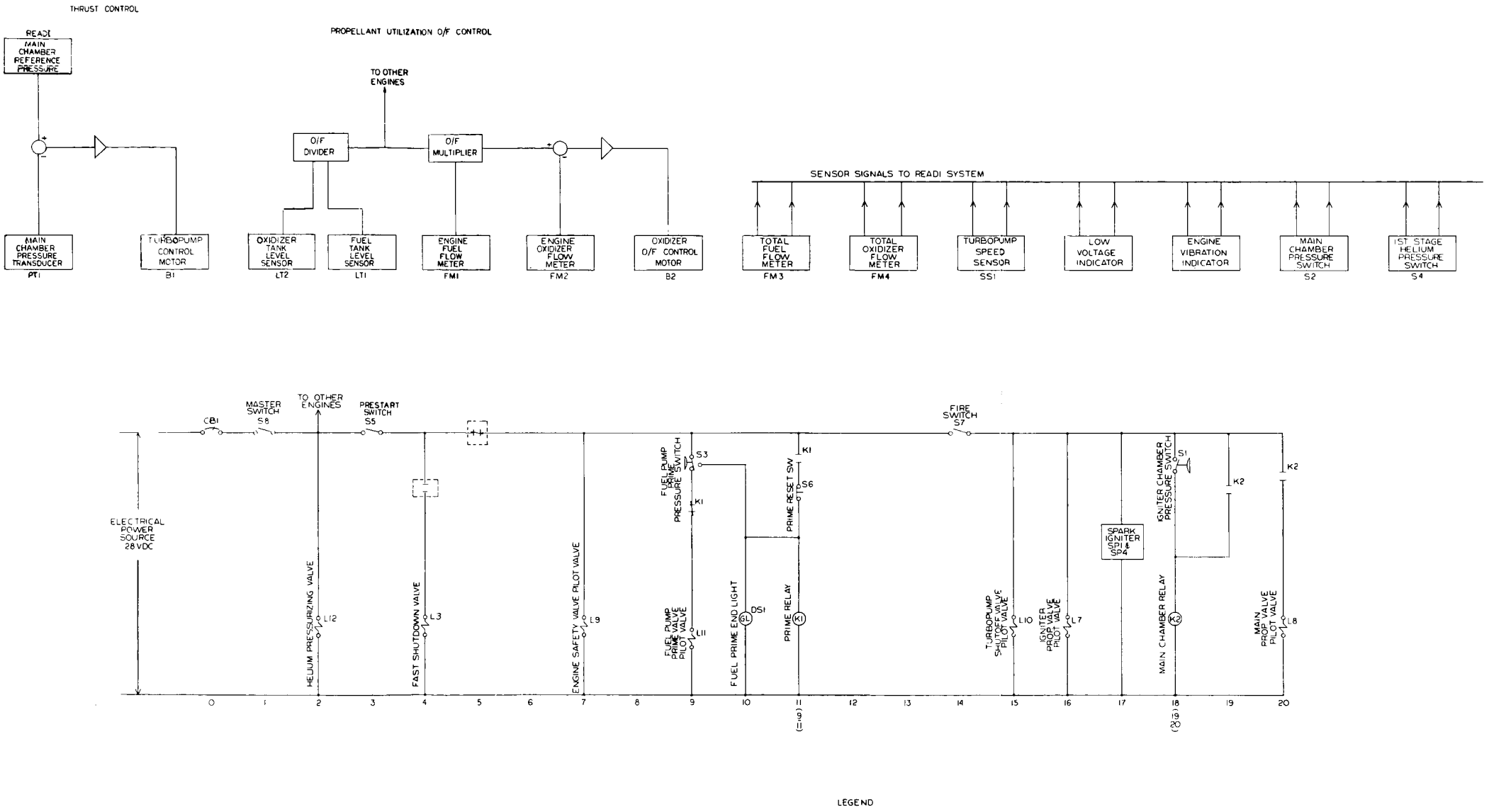


FIGURE G-2
READI MODEL ENGINE-
ELECTRICAL SCHEMATIC

APPENDIX G

READI MODEL ENGINE

G-1. INTRODUCTION

An engine configuration has been hypothesized to serve as a model on which the various READI concepts and configurations can be tried. Because of limitations of security and proprietary data, it was considered preferable to design a representative configuration than to work with a real engine. The engine chosen is a second and third stage 200,000-pound thrust LO_2-LH_2 engine. The essential features of the engine are given below. Fluid and electrical schematics appear in figures G-1 and G-2, respectively.

Thrust	200,000 pounds at altitude
Specific Impulse	420
Propellants	LO_2, LH_2
Cooling	Regenerative
Pumping	Turbopump with gas generator
Expansion Area Ratio	25:1
Mixture Ratio, Main Chamber	5:1
Mixture Ratio, Gas Generator	1:1
Rated Duration of Operation	400 sec
Chamber Pressure	600 psi
Pressurization	Helium start plus autogenous.

Note that in figure G-1 the whole propulsion system for a second stage is shown, since the READI model engine includes tankage, fuel and oxidizer pressurization systems, and control gas source, in addition to the liquid rocket engine. Table G-1 lists the pressure budget for a READI model engine at 100 percent thrust.

TABLE G-1

PRESSURE BUDGET
MODEL ENGINE
AT 100 PERCENT THRUST

Station No.	FLUID FLOWING	LOCATION	PRESSURE (PSIA)
1	Helium Gas	Helium Tank Exit	5000-750
2	Helium Gas	Exit 1st Stage Regulation	650
3	Helium Gas	Exit Helium Heat Exchanger (HE2)	600
4	Helium Gas	Exit TK1 Heat Exchanger (HE3)	550
5	Helium Gas	Exit 2nd Stage Regulation	55
10	- - - - -	Propellant Tankage	50
11	Liquid Fuel	Fuel Pump Inlet	35
12	Liquid Fuel	Fuel Pump Exit	920
13	Liquid Fuel	Exit Fuel Flow Meter (FM1)	910
14	Liquid Fuel	Cooling Jacket Inlets	900
15	Gaseous Fuel	Main Cooling Jacket Exits	750
16	Gaseous Fuel	Igniter Cooling Jacket Exit	810
17	Gaseous Fuel	Turbopump Control Valve Inlet	730
18	Gaseous Fuel	Turbopump Control Valve Exit	550
20	Gaseous Fuel	Main Prop Valve Exit	730
21	Gaseous Fuel	Igniter Prop Valve Exit	790
31	Liquid Oxidizer	Oxidizer Pump Inlet	35
32	Liquid Oxidizer	Oxidizer Pump Exit	990
33	Liquid Oxidizer	Oxidizer O/F Control Valve Exit	840
34	Liquid Oxidizer	Main Oxidizer Trim Orifice Exit	750
35	Liquid Oxidizer	Main Prop Valve Exit	730
36	Gaseous Oxidizer	Heat Exchanger (HE1) Exit	810
37	Gaseous Oxidizer	Turbopump Control Valve Inlet	790
38	Gaseous Oxidizer	Turbopump Control Valve Exit	550
39	Gaseous Oxidizer	Igniter Prop Valve Exit	790
41	Combustion Products	Igniter Chamber	660
42	Combustion Products	Main Thrust Chamber	600
43	Combustion Products	Turbine Gas Generator	460
44	Combustion Products	Turbine Exhaust	Ambient

The following provisions are included in the engine and are used in various decision processes:

- Tank safety values at each engine (U4)
- Redundancy in pressurization system
- Variable thrust ±20 percent by control of gas generator supply
- Variable 0/F for propellant management
- Separate ignitor chamber with safety interlock (not part of READI)
- Fast shutdown provision for certain malfunctions
- Restart capability.

The inclusion of some provisions like fast shutdown and variable thrust help the READI system in that they increase the alternate capabilities of READI. However, others, such as redundancy in pressurization and the igniter chamber interlock arrangement, make the system inherently more reliable and safe, which tends to reduce somewhat the value of READI. The premise is that both types of features will be incorporated in future engines employing a READI-type system.

G-2. MODEL ENGINE DETAILED DESCRIPTION

The following paragraphs describe the READI model engine in detail. The operational cycles of prestart, start, operate and shutdown are covered by tracing the flow sub-systems, i.e., fuel, oxidizer and helium. The control performance for thrust and oxidizer/fuel ratio controls is given at the end of the section.

A. GENERAL

The main thrust chamber and its igniter are regeneratively cooled with hydrogen. Propellants are fed to the engine pressurized by a turbopump. A single turbine is used which drives the fuel pump directly. The oxidizer pump is driven at roughly 1/3 turbine speed by means of gear reduction. The turbine is driven by combustion gases evolved in a bi-propellant gas generator which utilizes gaseous hydrogen and oxygen as propellants. The turbine exhaust gases are vented to ambient through a thrust recovery nozzle.

The net positive suction head (NPSH) required by the pumps is provided by a heated helium propellant tank pressurization system. The helium is heated by a heat exchanger incorporated in the nozzle extension of the main chamber. The propellants for the five engines and their associated turbine gas generators are contained in two tanks, one each for fuel and oxidizer. The helium required to produce the NPSH is stored in a tank contained within the fuel tank.

The main thrust chamber, which operates on liquid oxidizer and gaseous fuel, is lit by means of the thermal energy supplied by an igniter chamber, which operates on both gaseous oxidizer and fuel, as does the turbine gas generator. The igniter and turbine gas generator are lit by means of the thermal energy supplied by a spark plug. Two spark plugs are included in each for increased reliability. The gaseous oxidizer, required for igniter and turbine gas generator operation, is generated by bleeding liquid oxidizer from downstream of the oxidizer pump and passing it through a heat exchanger located around the turbine exhaust nozzle.

Aside from the normal on-off controls, the engine system contains controls for engine O/F ratio and thrust variability from 100 to 120 percent. The working medium for all pilot operated on-off controls is high pressure heated helium.

B. ENGINE OPERATIONAL CYCLES

1. Prestart

This cycle of operation is utilized to pressurize the engine systems and to prime the propellant pumps. The cycle is entered by closing the circuit breaker CB1, line 0, and the master switch S8, line 1. (Figure G-2) This will energize all circuits up to the prestart switch in each of the five engine systems. Any, or all, of the prestart switches S5, line 3, are now closed. The following will occur in the various fluid systems.

a. Helium System

The helium pressurizing valve solenoid L12, line 2, will be supplied current and the valve, U12, will be actuated to the open position. This will allow the high pressure helium to flow from the helium tank, TK1, and flow through the parallel first stage helium pressure regulators, RG1 and RG2. These regulators are redundant

in parallel for reasons of reliability and thus if either fails in the "locked-up" position, the other is sized to handle the maximum demands of the entire five engine system. After leaving these regulators the helium passes through the first stage regulator malfunction valves, U13 and U14. These valves are designed to close in the event either regulator fails in the wide open position. Check valves, CK1 and CK2, are provided so that in the event of an overpressurized condition in one of the parallel branches, the condition will not feed back into the other branch.

The helium has now passed the first stage regulation network and branches out to all five engines. In each engine system its path is the same and thus only one engine system need be discussed. The helium travels to the heat exchanger (HE2) located on the nozzle extension of the main thrust chamber. While passing through this heat exchanger the helium absorbs thermal energy so that NPSH can be provided more efficiently due to a higher helium pressurizing gas temperature. After leaving the heat exchanger, the helium travels back to the tankage section of the system. On the way, gas is tapped off, where required, to provide control gas for the five pilot valves in each engine system. Downstream of these tap-offs, the helium flow from all five engines rejoins in a common manifold. The manifold now travels through the helium tank, TK1, and a heat exchanger, HE3, is formed within the tank with a surface area sufficient to provide enough heat transfer to approximate an isothermal expansion of the helium leaving the tank going to the first stage of regulation. After leaving the heat exchanger, HE3, the helium passes through the second stage of regulation where its pressure is reduced to a level sufficient to provide an adequate NPSH for the propellant pumps. The second stage of regulation is a parallel redundant set-up exactly the same as the first stage of regulation discussed previously. Quadruple check valves are provided at the gas entrance to each propellant tank to preclude the possibility of inter-propellant mixing.

b. Oxidizer System

The engine safety valve pilot valve solenoid L9, line 7, will be supplied current and the valve, U9, will be actuated to the open position. This will allow control gas to flow into the actuating piston of the engine safety valve, U4, causing it to open. Oxidizer will flow from the oxidizer tank, TK2, under the influence of the helium gas pressurization and will branch out to all five engine systems. As all five engine oxidizer systems are the same, only one

will be discussed here. Oxidizer will pass through the now open engine safety valve, U4, and enter the oxidizer pump, TP2. After leaving this pump, the oxidizer flow will split up to three places:

(1) Main Chamber Oxidizer Flow - Oxidizer will flow to the normally closed (NC) main prop valve, U2. In the oxidizer portion of this valve a bleed port overboard is provided when the valve is in its normal position. Constant bleed of the oxidizer overboard during the prestart period will insure that the oxidizer pump, TP2, will be filled with liquid oxidizer when an engine start is made.

(2) Igniter Oxidizer Flow - Oxidizer will flow through the oxidizer heat exchanger, HE1, and up to the NC igniter prop valve, U1. The heat exchanger, HE1, absorbs heat from the turbine exhaust gases so that the igniter and turbine gas generator will operate on gaseous oxygen.

(3) Turbine Gas Generator Oxidizer Flow - Also, after leaving the oxidizer heat exchanger HE1, gaseous oxidizer will flow up to the NC turbopump shutoff valve U6.

c. Fuel System

Fuel will flow from the fuel tank, TK3, under the influence of the helium gas pressurization and will branch out to all five engine systems. As all five engine fuel systems are the same, only one will be discussed here. Fuel will flow through the now open engine safety valve, U4, and enter the fuel pump, TP1. After leaving this pump, the fuel flow will split up to two places:

(1) Fuel Prime Flow - The fuel pump prime valve pilot valve solenoid L11, line 9, will be supplied current and the valve, U11, will be actuated to the open position. This will allow control gas to flow into the actuating piston of the NC fuel pump prime valve, U5, causing it to open. Fuel, which has been converted from the liquid to the gaseous state due to heat transfer from the hardware comprising its flow path, will flow overboard through the opened valve,

U5. A pressure switch, S3, has been placed downstream of the valve, U5, and upstream of a fixed orifice. The fixed orifice is sized and the S3 pressure switch setting is such that when gaseous fuel is flowing overboard the pressure switch will remain in its normal (unactuated) position. When the associated hardware has been cooled down sufficiently such that the fuel pump, TP1, is filled with liquid fuel, liquid fuel will also begin to flow through the fuel pump prime valve, U5. As liquid fuel enters the fixed orifice, the pressure level upstream of the orifice will increase, causing the pressure switch, S3, to actuate. Actuation of this switch will discontinue current to the fuel pump prime valve pilot valve solenoid L11, line 9, closing the valve and illuminate the display signal DS1, line 10, indicating that the fuel pump is primed. Actuation of the S3 switch will also energize the prime relay K1, line 11, which will cause the normally open (NO) K1 contacts, line 11, to close, which will lock in the relay and also the NC K1 contacts, line 9, will open. The latter contacts are required as once the fuel pump prime valve U5 returns to its NC position, the pressure switch, S3, will also return to its normal position causing U5 to open again if the NC K1 contacts, line 9, are not included. The fuel pump, TP1, will remain in the primed condition for a reasonable period of time after the display signal DS1, line 10, has been illuminated. During this period of time, the engine can enter the "fire" mode. If this period of time has been exceeded when the engine is required to be started, then the fuel pump, TP1, must be primed again. This is accomplished by depressing the momentary break prime reset switch S6, line 11. This will discontinue current to the prime relay K1, line 11, and cause both of its contacts (lines 9 and 11) to return to their normal positions. The fuel pump, TP1, will now be primed again as described above.

(2) Engine Fuel Flow - There is sufficient hardware mass in the engine system so that the fuel will be in the gaseous form when the engine is required to start. When the fuel reaches the engine, it branches out to two places:

(a) Igniter Fuel Flow - Fuel passes through the igniter chamber (CH1) cooling jacket and flows up to the NC igniter prop valve, U1.

(b) Main Chamber and Gas Generator Fuel Flow - Fuel passes through the main chamber (CH2) cooling jacket and then splits up to two places:

- Turbine Drive Gas Generator Fuel Flow - Upon leaving the main chamber cooling jacket, fuel flows up to the NC turbopump shutoff valve, U6.
- Main Chamber Fuel Flow - Upon leaving the main chamber cooling jacket, fuel also flows up to the NC main prop valve, U2.

The engine is now ready to be started.

2. Start

The start cycle is entered by closing the start switch S7, line 14. The fuel prime end light DS1, line 10, must be illuminated when the start attempt is made. Closing the fire switch will initiate three events simultaneously:

- The spark ignitors SP1 and SP2, line 17, for the main thrust chamber igniter, CH1, will be energized, and spark ignitors SP3 and SP4, line 17, for the turbine gas generator, CH3, will be energized.
- The igniter prop valve pilot valve solenoid L7, line 16, will be energized causing the valve U7 to actuate to the open position. This will allow control gas to flow into the actuating piston of the igniter prop valve, U1, causing it to open.
- The turbopump shutoff valve pilot valve solenoid L10, line 15, will be energized causing the valve U10 to actuate to the open position. This will allow control gas to flow into the actuating piston of the turbopump shutoff valve, U6, causing it to open.

Propellants will enter the main thrust chamber igniter, CH1, under the influence of suppression head. The propellants will mingle and be ignited by the thermal energy supplied by the spark plugs, SP1 or SP2.

Propellants will enter the turbine gas generator, CH3, under the influence of suppression head. The propellants will mingle and be ignited by the thermal energy supplied by the spark plugs, SP3 or SP4. After leaving the turbine, the turbine drive gases pass through a thrust recovery nozzle to ambient.

As the turbine comes up in speed, the igniter chamber pressure will rise. The normally open igniter chamber pressure switch S1, line 18, is set to actuate at a pressure level sufficiently high so that proper operation of the igniter and a proper bootstrap of the turbine has been insured. Once the switch S1, line 18, actuates, the main chamber relay K2, line 18, will be energized. This will cause the relay's normally open K2 contacts, line 19, to close locking in the relay around the pressure switch S1, line 18. This is done so that possible chattering of the switch contacts will not effect engine operation. In addition, the normally open K2 contacts, line 20, will close. This will allow current to energize the main prop valve pilot valve solenoid L8, line 20. This in turn will cause the valve U8 to open allowing control gas to enter the actuating piston of the main prop valve, U2. A fixed orifice is placed in the control gas line so that the main prop valve, U2, will open at a controlled, safe rate.

Propellants will now be allowed to flow through the main prop valve, U2, and into the main thrust chamber, CH2. These propellants will then mingle and be ignited by the thermal energy supplied by the main thrust chamber igniter, CH1.

3. Operation

During operation of the engine, the READI system can run any or all of the engines over a range of O/F ratio from 4.5 to 5.5 by sending the proper signal to the oxidizer O/F control valve, U25. This valve is driven by an electric motor through a gear reduction.

In addition, during operation of this engine, the READI system can vary the thrust of any or all of the engines over a range of 100 to 120 percent by sending the proper signal to the turbopump control valve, U24.

4. Shutdown

Shutdown is accomplished by opening the fire switch S7, line 14. This will discontinue current to the turbopump, igniter, and main chamber pilot valve solenoids: L10, L7, and L8, lines 15, 16,

and 20, respectively. The control gas is vented from the actuating piston of the main prop valve, U2, at a controlled rate, by means of a fixed orifice in the vent line, so that the main prop valve, U2, will close at a slow rate. The actuating piston of the igniter prop valve, U1, has a control gas accumulator built into it so that in conjunction with a fixed orifice in the vent line a predetermined delay in igniter firing termination, relative to main chamber firing termination, can be afforded. In this way, any residual propellants in the main chamber will be eliminated by the extended firing of the igniter.

The engine will now be in the prestart condition and is ready for immediate restart.

5. Extended Shutdown

If the engine is to go through an extended shutdown, then the prestart switch S5, line 3, and the circuit breaker CB1, line 0, are to be opened also.

6. Fast Shutdown

If for some reason it is required that the main thrust chamber be shut down quickly, then this can be accomplished by opening the fire switch S7, line 14, or by opening the READI signal, line 5. In addition, the READI signal, line 4, is to be closed, which will energize the fast shutdown valve solenoid L3, line 4. This will cause valve U3 to open and vent the actuating piston of the main prop valve, U2, without the use of the fixed orifice pneumatic timer located in the vent line of the main prop valve pilot valve, U3. Thus the main prop valve, U2, and consequently the main thrust chamber, CH2, will shut down quickly.

7. Immediate Restart

Immediate restart is accomplished as described in paragraph 2.

8. Restart After an Extended Shutdown

If CB1, S8, or S5, lines 0, 1, and 3, respectively, are open, then the procedures as outlined in paragraphs 1 and 2 are applicable.

If only S7, line 14, is open, then the prime reset switch S6, line 11, must be pushed, and upon illumination of DS1, line 10, the procedure outlined in paragraph 2 can be followed.

C. PROPELLANT UTILIZATION CONTROL

The propellant utilization control receives a signal from each propellant tank indicating the amount of propellant remaining. An O/F divider translates these two signals into an output signal to all engines which defines the O/F required for both propellant tanks to empty simultaneously. The signal is limited to the values corresponding with the allowable O/F tolerance established for the engines. An O/F multiplier for each engine combines this "required O/F" signal with a signal from the engine fuel flowmeter, and provides an output which indicates the oxidizer flow necessary to maintain the O/F ratio demanded by the O/F divider. This "required oxidizer flow" signal is combined with the engine oxidizer flowmeter output to produce an error signal which is a measure of the change in oxidizer flow necessary for the engine to run at the O/F demanded. The error signal is amplified and fed to the oxidizer O/F control motor, which positions the oxidizer control valve so as to reduce the error signal to zero. Thus, individual engine O/F ratio and proper utilization of propellants for the entire engine cluster are maintained continuously.

Appendix H
ENGINE CORRECTIVE ACTIONS

APPENDIX H

ENGINE CORRECTIVE ACTIONS

H-1. INTRODUCTION

READI functions to sense the condition of the propulsion system and take corrective action to reduce the crew risk and the mission risk. The action may be implemented directly by READI or initiated through the crew.

Without corrective action the READI model engine can degrade to one of four categories, which are representative of large rocket engines in current use and in development.

- failure to start	0.001
- premature safe shutdown	0.002
- off-design operation	0.003
- explosion	0.004
	0.010

The first two categories lead to loss of required vehicle velocity increment. Off-design operation can cause sufficient loss of velocity increment to use up all of the corrective ability of the stage and can lead to failure of the stage. The explosion category implies vehicle destruction and loss of the crew. The corrective actions taken by READI must shift the systems from the above states to a normal or near normal state.

Loss of thrust may be compensated for by:

- restarting the engine
- designing the mission so that the objectives can be achieved with one engine out and increased burning time
- increasing thrust on remaining engines to regain a substantial portion lost with one engine out
- combinations of the above.

Off-design performance due to propellant overboard leakage can, in most cases, be eliminated by shutting down. Much of the off-design category is associated with degradation-type failures for which little can be done, the best choice being to do nothing.

The explosion category presents the most serious threat. The action required in most cases is engine shutdown. In some cases, such as combustion instability and failures which involve accumulation of propellant, the engine must be shut down at a rate significantly faster than normal.

Figure H-1 shows the transitions which occur when appropriate action is taken. The results of the actions are to shift the system toward the normal or near normal state which allows completion of the mission and saves the crew. Figure H-1 shows only engine states, however. The READI system evaluation procedure describes vehicle operational states in terms of velocity errors which are calculated from the losses in engine performance resulting from the engine states, with and without corrective action.

H-2. COMPENSATION FOR LOST THRUST

A. RESTART

A number of current real engines, as well as the model engine used for analysis and evaluation of the READI concepts, are capable of restarting in flight. There are numerous failure instances when a restart might be tried, but the explosion hazard is high in many of these. For the model engine the restart attempt was programmed for pump cavitation (ox or fuel) and for combustion instability (after successful shutdown).

B. ENGINE-OUT CAPABILITY - EXTRA BURNING TIME

In multi-engine stages with five or more engines, one attractive possibility is simply to allow the remaining engines in the cluster to burn longer, thus using up all of the propellants. However, a slight reduction in payload must be allowed. The payload reduction results, in effect, from the addition of an extra engine to the stage and a trajectory penalty. The trajectory penalty results because it is necessary for the vehicle to follow compromise trajectories with either all engines running or with one engine out.

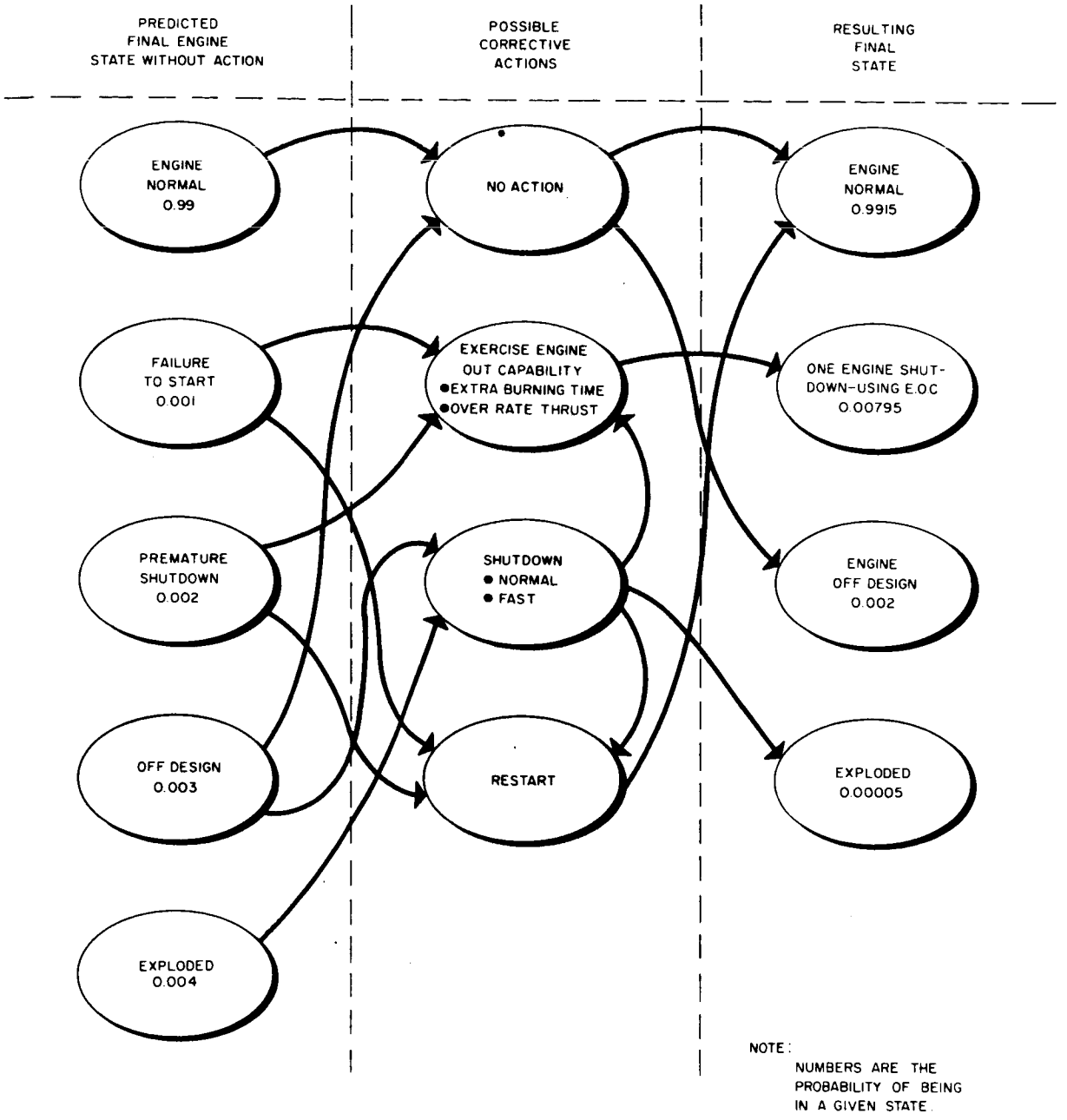


FIGURE H-1
ENGINE MODEL

The potentialities and limitations of vehicles and missions which allow extra burning time to achieve engine-out capability have been calculated in some detail by Rocketdyne. The results of the analyses, which treat the reliability, mission and thrust vector control problems, have been summarized in a Rocketdyne report[1].

C. ENGINE-OUT CAPABILITY - ENGINE OVERRATING

Most liquid rocket engines can, and have, been run above their design point thrust in the course of development testing. There are examples of engines which have been uprated in thrust over a period of years with relatively minor changes. Engines which employ bootstrap cycles (including the READI model engine) can be overrated simply by increasing the bootstrap flow. Pressurized engines can be overrated by opening up restrictions between the tanks and thrust chamber. Alternately, tank pressure can be increased to the maximum allowable level. A +20-percent thrust increment has been used in all READI analyses.

The ground rule assumption in overrating is that the model engine is nominally a fixed thrust device; overrating is to be used only in emergencies. By overrating the engine some of the design safety factor is "used up". The probabilities of some engine failures will increase because of the increase in overlap of component stress and strength distributions. A distinction is, therefore, drawn between uprating and overrating since the latter implies a calculated increase in risk.

A detailed analysis of some of the representative components of a liquid rocket engine, when subject to overrating, may be found in Appendix J. In Appendix J, curves are presented showing the percent probability of failure versus percent increase in thrust for pump case stress, wheel stress, cavitation limit, exhaust manifold stress, and chamber heat transfer limit for various ground rule assumptions.

Implementation of thrust change can vary considerably in difficulty, depending on the engine. An engine which is already designed for variable thrust operation is, of course, simple to handle. If the engine has a constant thrust controller, the change can be introduced by varying the thrust feedback reference. It is a common engine test

- - - - - - -

[1] R-3553 "Engine-Out Capability", Rocketdyne Corp., April 1962, Confidential

practice to install two-step or continuous valves in propellant bootstrap lines. Similar valve designs can easily be integrated into most current liquid rocket engines. The main cost would not be the hardware but the analyses and tests needed to verify the change. The READI model engine includes a two-position motor-driven value, U24, which is used to change thrust from nominal to 120 percent and return.

H-3. SHUTDOWN

The most used corrective action is shutdown. Fortunately, all liquid rocket engines have this capability. There are some failures which lead to explosion that propagate from the incipient level to destruction very rapidly. The main propellant shut-off valves of most large liquid rocket engines include a hydraulic bleed network which restricts the speed with which the valve can shut. The purpose of this arrangement is to reduce the hydraulic hammer effect on the piping system that results if the valve is allowed to shut at the maximum speed within its capability. However, this controlled closure allows the engine to proceed to destruction in some cases. A "fast shutdown" valve is, therefore, hypothesized, the purpose of which is to shut the main propellant valve (or valves) at a fast rate.

As in the engine overrating concept, the assumption is that the fast shutdown is used only in case of a malfunction. The closing time is cut down to an interval which is the shortest which can be tolerated based on increase in risk of bursting the inlet plumbing versus the risk of engine explosion resulting from the malfunction. Figure H-2 shows how the pressure surge increases as closing time is cut down for a typical fuel propellant valve[2].

A fast shutdown valve, U8, has been included in the READI model engine. The tie-in of this valve with programmed decisions is discussed in the next section.

H-4. COMPARISON OF CORRECTIVE ACTIONS

To get an analytical insight into the value of the alternates which might be added to the model engine, a series of mission loss evaluations was run. The variable which was perturbed was the programmed decision for each malfunction area. This amounts to an evaluation of a series of perfect READI systems with variable decisions.

- - - - - - -

[2]George Rich, "Hydraulic Transients", McGraw Hill, 1951, p. 24.

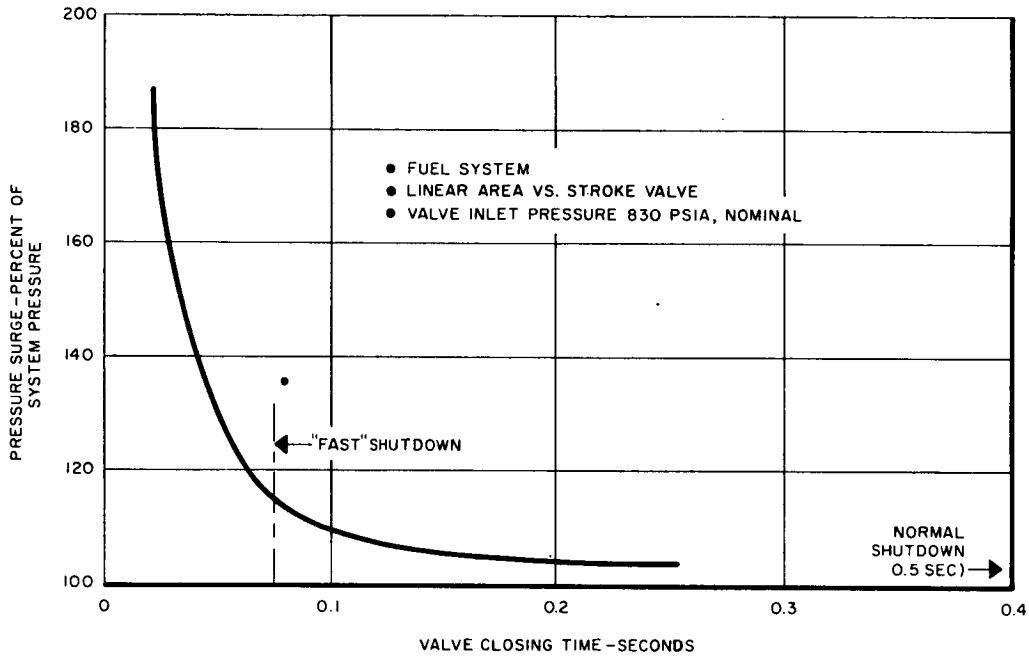


FIGURE H-2

PRESSURE SURGE VERSUS MAIN PROPELLANT VALVE CLOSING TIME

The programmed decisions were built up according to a logical scheme of adding alternate capabilities to the engine one at a time. Table H-1 shows the manner in which systems were built up, and in the lower part the resulting programmable decisions. The best choice decision for each malfunction area by engine phase is shown in table H-2.

The considerations in choosing the best decision to program for a given malfunction and engine phase are:

- the losses resulting from the failure without corrective action, particularly the explosion probability
- the response time required
- the available decisions which can be programmed.

The optimum decision changes with the alternates that are available. For instance m4, fuel pump cavitation, would make use of the following sets of decisions as various degrees of freedom are added to the engine. From table H-2 the following are found during start and operate phases:

System	A	B	C	D	E	F	G	H
Decision No.	2	2	11	11	4	4	6	6

D2 = shutdown

D11 = shutdown, attempt restart (added restart to A)

D4 = shutdown, run other engines at 120-percent thrust (added overrating to A)

D6 = shutdown, run other engines at 120-percent thrust, attempt normal restart; if successful, reduce thrust on other engines to 100 percent.

For m16, combustion instability, the best decision changes with every change to the engine.

System	A	B	C	D	E	F	G	H
Decision No.	2	5	11	12	4	13	6	7

H-5. TIME INTERVAL FOR CORRECTIVE ACTION

The time interval which may be allowed for corrective action depends on how fast the engine condition propagates from the

Table H-1

BUILD-UP OF ALTERNATE ACTIONS AND RESULTING DECISIONS

System	Action	1	2	3	4	5	6	7	8	9	10
		No Action	Shut Down	Fast Shut-down	Restart	Fast Restart	Run at 80% Thrust	Run All Engines at 120% Thrust	Return to 100% Thrust	Run Other Engines at 120% Thrust	Run Other Engines at 105% Thrust
A		X	X								
B		X	X	X							
C		X	X		X						
D		X	X	X	X	X					
E		X	X					X			
F		X	X	X				X			
G		X	X		X			X	X	X	
H		X	X	X	X			X	X	X	
I		X	X				X	X			X
J		X	X		X		X	X	X	X	X
K		X	X	X	X	X	X	X	X	X	X
Decision Number											
1		1									
2			1								
3								1			
4			1					1			
5			1	1							
6			1		2				[3]	1	
7			1	1	2				[3]	1	
8			[2]				1	[2]			1
9							1				1
10			1	1		[2]					
11			1								
12			1	1							
13			1	1				1			

Note:

[1] Number indicates the order in which actions, if any, are taken

[2] ☐ Indicates that the action in the box is conditional upon the response of the engine to the previous action

TABLE H-2

PROGRAMMED DECISIONS FOR VARIOUS ENGINE SYSTEMS

m	Area	PM Probability of Malfunction	Operational Mode	System A	B	C	D	E	F	G	H
1	Loss of Helium	0.00022	Prestart	2	2	2	2	2	2	2	2
		0.00014	Start	2	2	2	2	2	2	2	2
	a. U12 closed	0.00012	Operation	2	2	2	2	2	2	2	2
	b. U17 opened	0.00012	Shutdown	2	2	2	2	2	2	2	2
	c. U18 opened	0.00018	Restart	2	2	2	2	2	2	2	2
2	Low Fuel Flow	0.00010	Prestart	1	1	1	1	1	1	1	1
	a. Clogged injector	0.00020	Start	1	1	1	1	1	1	1	1
		0.00057	Operation	2	2	2	2	4	4	4	4
	b. Fuel leakage	-------	Shutdown	1	1	1	1	1	1	1	1
	(Stations 11-12)	0.00010	Restart	1	1	1	1	1	1	1	1
3	Low Ox Flow	0.00005	Prestart	1	1	1	1	1	1	1	1
	a. Clogged injector	0.00011	Start	1	1	1	1	1	1	1	1
		0.00038	Operation	1	1	1	1	4	4	4	4
	b. Ox leakage	-------	Shutdown	1	1	1	1	1	1	1	1
	(Stations 31-32)	-------	Restart	1	1	1	1	1	1	1	1
4	Loss of Fuel to One Engine	-------	Prestart	1	1	1	1	1	1	1	1
		0.00032	Start	2	2	12	12	4	4	6	6
	a. Pump Cavitation	0.00018	Operation	2	2	12	12	4	4	6	6
		-------	Shutdown	1	1	1	1	1	1	1	1
		0.00032	Restart	1	1	12	12	4	4	6	6
5	Loss of Ox to One Engine	-------	Prestart	1	1	1	1	1	1	1	1
		0.00013	Start	2	2	12	12	4	4	6	6
	a. Pump Cavitation	0.00007	Operation	2	2	12	12	4	4	6	6
		-------	Shutdown	1	1	1	1	1	1	1	1
		0.00013	Restart	1	1	12	12	4	4	6	6
6	Low Pump Speed	-------	Prestart	1	1	1	1	1	1	1	1
	a. B1 or U24 Stuck	0.00020	Start	1	1	1	1	1	1	1	1
	b. GG Structural failure	0.00152	Operation	1	1	1	1	4	4	4	4
	c. Gear or Bearing failure	-------	Shutdown	1	1	1	1	1	1	1	1
	d. Pump Structural failure	0.00020	Restart	1	1	1	1	1	1	1	1
	e. Turbine or Nozzle erosion										
	f. Eroded oxing, clogged fueling (Low CG O/F)										
7	No Pump Speed	-------	Prestart	1	1	1	1	1	1	1	1
	a. U6 or U10 closed	0.00019	Start	2	2	2	2	4	4	4	4
	b. GG Structural failure	0.00060	Operation	2	2	2	2	4	4	4	4
	c. Gear or Bearing failure	-------	Shutdown	1	1	1	1	1	1	1	1
	d. Pump Structural failure	0.00019	Restart	2	2	2	2	4	4	4	4
	e. Turbine or Nozzle erosion										
8	Premature Gas Generator Flow	0.00010	Prestart	2	2	2	2	2	2	2	2
		-------	Start	1	1	1	1	1	1	1	1
	a. U6 open	-------	Operation	1	1	1	1	1	1	1	1
	b. U10 open	0.00009	Shutdown	2	2	2	2	2	2	2	2
	(Turbopump Shutoff Valve)	-------	Restart	1	1	1	1	1	1	1	1
9	Loss of, or Low, Electrical Power	0.00003	Prestart	2	2	2	2	2	2	2	2
		0.00003	Start	2	2	2	2	2	2	2	2
		0.00003	Operation	2	2	2	2	2	2	2	2
		0.00003	Shutdown	2	2	2	2	2	2	2	2
		0.00003	Restart	2	2	2	2	2	2	2	2
10	Loss of Ox & Fuel	0.00018	Prestart	2	2	2	2	2	2	2	2
	a. U4 closed	0.00007	Start	2	2	2	2	4	4	4	4
	b. U9 closed	0.00007	Operation	2	2	2	2	4	4	4	4
	(Tank Safety Valve)	0.00007	Shutdown	2	2	2	2	2	2	2	2
		0.00012	Restart	2	2	2	2	4	4	4	4
11	Premature Igniter Flow	0.00006	Prestart	2	2	2	2	2	2	2	2
	a. U1 open	-------	Start	1	1	1	1	1	1	1	1
	b. U7 open	-------	Operation	1	1	1	1	1	1	1	1
	(Igniter Prop. Valve)	0.00013	Shutdown	2	2	2	2	2	2	2	2
		-------	Restart	1	1	1	1	1	1	1	1
12	Loss of Main Chamber Flow	-------	Prestart	1	1	1	1	1	1	1	1
		0.00018	Start	2	2	2	2	4	4	4	4
	a. U2 closed	0.00006	Operation	2	2	2	2	4	4	4	4
	b. U8 closed	-------	Shutdown	1	1	1	1	1	1	1	1
	(Main Prop. Valve)	0.00010	Restart	2	2	2	2	4	4	4	4
13	Premature Main Chamber Flow	0.00005	Prestart	2	5	2	11	2	5	2	11
		0.00005	Start	2	5	2	11	2	5	2	11
	a. U2 open	-------	Operation	1	1	1	1	1	1	1	1
	b. U8 open	0.00010	Shutdown	2	5	2	11	2	5	2	11
	(Main Prop. Valve)	0.00005	Restart	2	5	2	11	2	5	2	11
14	No Fuel Prime	0.00019	Prestart	2	2	2	2	2	2	2	2
	a. U11 closed	-------	Start	1	1	1	1	1	1	1	1
	b. U5 closed	-------	Operation	1	1	1	1	1	1	1	1
	(Prime Valve)	-------	Shutdown	1	1	1	1	1	1	1	1
		-------	Restart	1	1	1	1	1	1	1	1
15	Premature Fast Shutdown	0.00003	Prestart		2		2		2		2
		0.00003	Start		2		2		4		4
	a. U3 open	0.00003	Operation		2		2		4		4
		0.00003	Shutdown		2		2		2		2
	(Fast Shutdown Valve)	0.00003	Restart		2		2		4		4
16	Vibration	-------	Prestart	1	1	1	1	1	1	1	1
	(Rough Combustion)	0.00135	Start	2	5	12	13	4	14	6	7
		0.00045	Operation	2	5	12	13	4	14	6	7
		-------	Shutdown	1	1	1	1	1	1	1	1
		0.00120	Restart	2	5	12	13	4	14	6	7
17	High Fuel Flow	-------	Prestart	1	1	1	1	1	1	1	1
	a. Chamber Burnout	-------	Start	1	1	1	1	1	1	1	1
	b. Injector erosion	0.00060	Operation	2	2	2	2	4	4	4	4
	c. External leakage	-------	Shutdown	1	1	1	1	1	1	1	1
	(Chamber area)	-------	Restart	1	1	1	1	1	1	1	1
18	High Ox Flow	-------	Prestart	1	1	1	1	1	1	1	1
	a. Injector erosion	-------	Start	1	1	1	1	1	1	1	1
	b. External leakage	0.00045	Operation	2	2	2	2	4	4	4	4
	(Chamber area)	-------	Shutdown	1	1	1	1	1	1	1	1
		-------	Restart	1	1	1	1	1	1	1	1
19	Low Fuel Flow	-------	Prestart	1	1	1	1	3	3	3	3
	(All Engines)	-------	Start	1	1	1	1	3	3	3	3
	a. QD2 open	0.00003	Operation	1	1	1	1	3	3	3	3
	b. U19 or U21 open	-------	Shutdown	1	1	1	1	3	3	3	3
	c. Line leakage	-------	Restart	1	1	1	1	3	3	3	3
20	Engine Compartment Fire	-------	Prestart	2	2	2	2	2	2	2	2
		-------	Start	2	2	2	2	4	4	4	4
	a. Turbine Exhaust	0.00040	Operation	2	2	2	2	4	4	4	4
	b. Duct Failure	-------	Shutdown	2	2	2	2	2	2	2	2
		-------	Restart	2	2	2	2	4	4	4	4
21	Off Design Gas Generator O/F	-------	Prestart	1	1	1	1	1	1	1	1
		0.00015	Start	2	2	2	2	4	4	4	4
	a. Clogged injector	0.00030	Operation	2	2	2	2	4	4	4	4
	b. Injector erosion	-------	Shutdown	1	1	1	1	1	1	1	1
	c. External leakage	0.00015	Restart	2	2	2	2	4	4	4	4
	d. HE1 Burnthrough										
22	Low Ox Flow	-------	Prestart	1	1	1	1	3	3	3	3
	(All Engines)	-------	Start	1	1	1	1	3	3	3	3
	a. QD1 open	0.00003	Operation	1	1	1	1	3	3	3	3
	b. U20 or U22 open	-------	Shutdown	1	1	1	1	3	3	3	3
	c. Line leakage	-------	Restart	1	1	1	1	3	3	3	3

incipient level to a "dangerous" level. Dangerous level implies high probability of explosion or loss of thrust. The lags in the correction loop are:

Δt_t = lag associated with the build-up of a sensed variable (or variables) to a threshold which permits identification of engine condition

Δt_s = lag associated with the sensor and connecting lines

Δt_p = READI electronic processing time

Δt_c = correction time which involves lags due to valves and engine response.

The "allowable" time interval, Δt_a, should be greater than the lags in the correction loop:

$$\Delta t_a > \Delta t_t + \underbrace{\Delta t_s + \Delta t_p}_{\text{READI system}} + \Delta t_c + \text{margin}$$

The Δt_t is generally very short; about one to five milliseconds is a representative range. The sensor lags are about the same or less if a proper transducer selection and installation have been made. An exception is the fire detector, which for some types has a lag of over one second. The dominant lag is Δt_c because of the controlled closing time built into the main propellant valves. For the READI model engine, shutdown requires from 300 to 400 milliseconds, while thrust changes can be accomplished in 100 milliseconds or less. Restart without priming requires 1500 milliseconds and the prime operation can add up to 20 seconds on a restart.

An estimate of allowable READI processing time, Δt_p, for each malfunction area is shown in table H-3. In the few cases where the Δt_c lag exceeds Δt_a the following rule was applied: the Δt_p lag is given as 5 percent of Δt_c, or 1/2 of the probable uncertainty in Δt_c which is generally about ±10 percent.

Table H-3

MAXIMUM ALLOWABLE READI PROCESSING TIME
(All times in milliseconds)

Malf. Area m	Response of Engine Δt_c	Allowable Time for Correction Δt_a	Estimated Max. Processing Time Allowed[1] Δt_p
1	500	2000	1500
2	500	2000	1500
3	500	2000	1500
4	<1	50	50
5	<1[2]	50	50
6	500	5000	4500
7	<1[2]	100	100
8	500	1000	500
9	500	2000	1500
10	<1[2]	100	100
11	500	1000	500
12	50	50	2.5[3]
13	80	30	4[3]
14	500	2000	1500
15	500	2000	1500
16	80	Unknown, but very small	4[3]
17	500	1000	500
18	500	1000	500
19	100	2000	1900
20	500	1000[4]	25[3]
21	500	1000	500
22	100	2000	1900

Notes:

[1] The sensor lag must be subtracted from Δt_p, but it is generally $\approx$5 msec

[2] Time to extinguish spark plugs

[3] 5% of Δt_a, or 1/2 of the probable uncertainty in Δt_c which is generally about ±10%
2 millisec sensor response required for m 12 and m 13

[4] Sensor response time ~1000 to 2000 msec.

Appendix I

ANALYSIS OF THE PROPULSION SYSTEM IN SUPPORT OF READI DESIGN

APPENDIX I

ANALYSIS OF THE PROPULSION SYSTEM IN SUPPORT OF READI DESIGN

I-1. INTRODUCTION

The READI equipment must accomplish two objectives:

- determine the condition of the engine
- initiate the best alternate action for a given condition. It is necessary therefore to first analyze the engine (i. e. propulsion system) and formulate various mathematical models which describe the system in its normal and failed conditions.

One of the most used models is a statistical failure model: most of this Appendix deals with the considerations and approach in developing this statistical model. A number of analyses were performed which are aimed at developing models of the engine when operating under failed or off-design conditions. Typical of this type of analysis done on the READI model engine were calculations of the time to accumulate a critical quantity of propellant in the thrust chamber, magnitude of pressure surge in propellant lines for fast shut down, and calculation of increase in engine failure rates with increased thrust. Analyses of this kind would increase by orders of magnitude in the design of a READI for a real engine. However, the framework for much of the work is already available for real engines.

I-2. STATISTICAL MODEL

In setting up a statistical model of the engine it is first necessary to perform a failure analysis on the engine to pinpoint failure sources and trace failure effects. A sample of part of the failure analysis performed on the representative engine is shown in table I-1. The format used is the standardized one evolved by MSFC[1] for documenting failure effects analyses on real engines and vehicles.

- - - - - - -

[1] NASA, MSFC Document MTP-P & VE-E-62-2, "A Generalized Approach for Systems Design and Analysis and Selection of Components for Automation".

The failure effects analysis is pursued to the final engine state which results without corrective action. The list of final states below covers all situations which can occur in the READI model engine for second stage operation.

- failure to start 0.001
- premature, safe shut down 0.002
- explosion 0.004
- severe off-design operation 0.003

For a stage requiring restart, two more states are defined:

- abnormal and/or dangerous condition after shutdown
- failure to restart.

Some arbitrary classifications of real situations are necessary to boil all of the failures down to only four categories. For instance, explosions are implied to be severe enough to lead eventually to vehicle destruction.

One way of organizing the analysis is to draw a failure network or tree. At the top of the tree are noted all of the possible failures which may occur in the propulsion system and at the bottom are several sinks or bases which are the final failure states mentioned above (figure I-1).

As the statistical analysis proceeds, it is possible to select malfunctions and small groups of malfunctions for which representative data is available and which are statistically independent. Statistical independence implies only that in figure I-1, one failure does not lead to another. For instance, 4 and 4' are related to each other in the failure process; therefore, 4' is not an appropriate malfunction area to be included in the m1, m2, m3, etc., group. For example, in the analysis of the representative engine, m7, "No Pump Speed" includes unrelated failures such as valve U6 or U10 stuck closed, turbopump gear/bearing failures, turbopump structural failure, and gas generator rupture.

It is desirable from the standpoint of obtaining statistical independence of failures, and for early warning, to separate the failures down to an elemental level. However, several considerations precluded this approach. Data is not generally obtainable on the elemental failures, and the bookkeeping part of the analysis increases in proportion to the number of failures. Therefore, in most areas of the engine a number of failures which lead to the same failure effect are

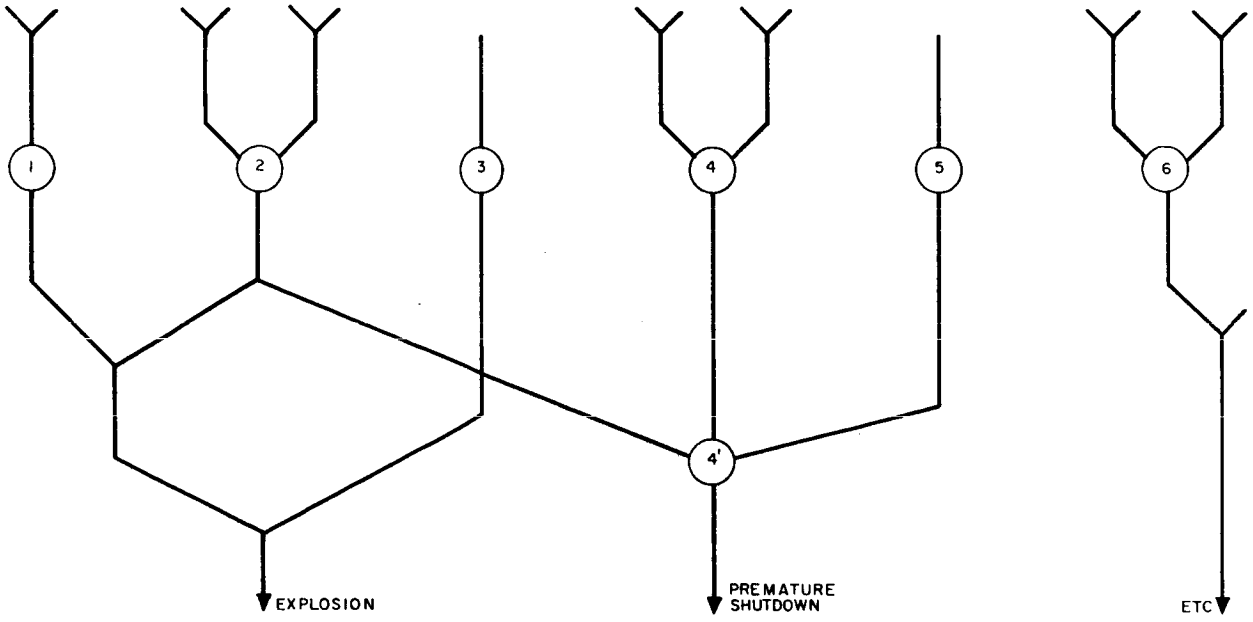


FIGURE I-1
FAILURE TREE SHOWING MALFUNCTION DEFINING LEVEL

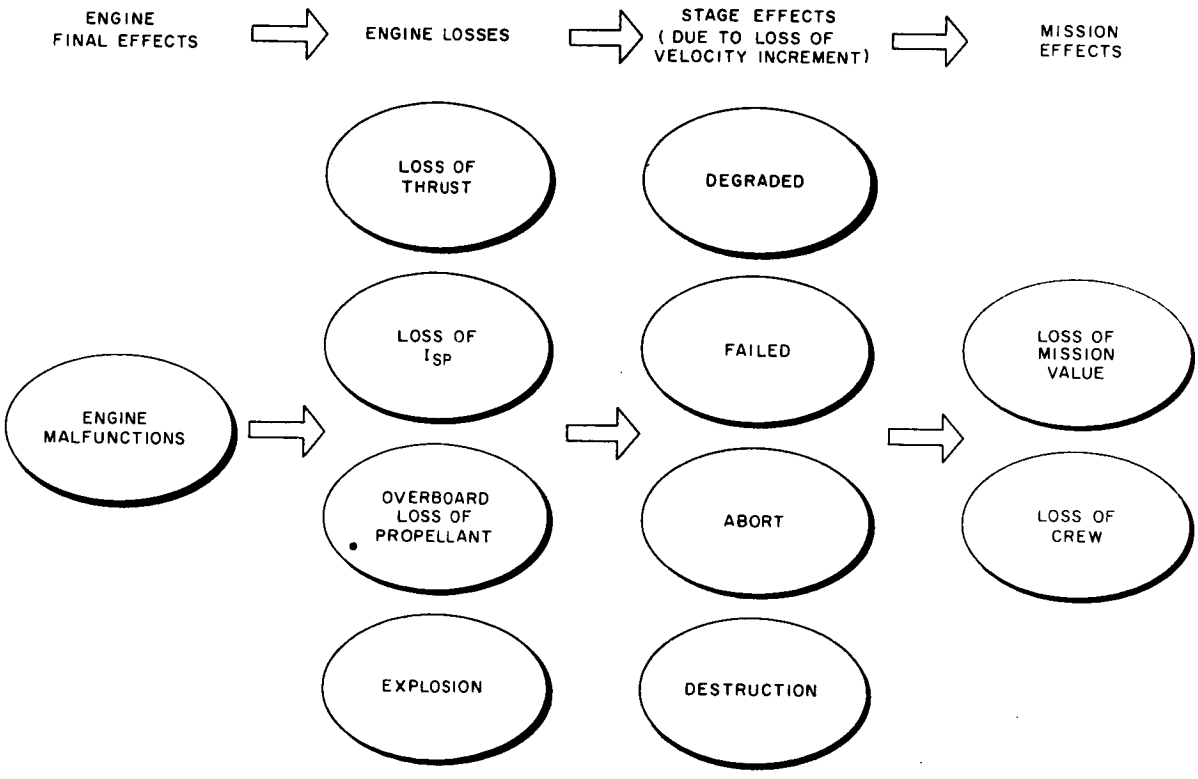


FIGURE I-2
PROPAGATION OF ENGINE MALFUNCTIONS
TO MISSION EFFECTS

TABLE I-1 FAILURE EFFECT ANALYSIS MODEL ENGINE (SAMPLE)

Item	**	Drawing Number	Elect. Ref. Desig.	Function	Failure Type	Failure Effect on Subsystem Performance	Failure Effect on Stage	Failure Effect on Vehicle
2. Fuel and Oxidizer Main Prop Valve-U2 or Main Prop Valve Pilot Valve - U8				Provides bi-propellant flow to main chamber	1. Inoperative-stuck closed			
					a) Prestart	None. During this phase of operation the valve is normally closed.	A) None B) None	A) None B) None
					b) Start	LOSS OF ENGINE: The main chamber will not start or will shutdown.	A) None B) None: Redundancy is provided by the remaining cluster of chambers.	A) None B) None
					c) Operation	LOSS OF ENGINE: The main chamber will shut down.	A) None B) None: Redundancy provided	A) None B) None
					d) Shutdown	None: Same as 2. 1. a.	A) None B) None	A) None B) None
					2. Inoperative stuck open			
					a) Prestart	POSSIBLE LOSS OF ENGINE: Both propellants will flow to the main chamber prematurely. If a critical quantity of propellants accumulate, a destructive pressure surge may occur when the igniter fires.	A) None: Not operational prior to launch. In addition, the propellant tank safety valve (U4) and the helium pressurizing valve (U12) are closed prior to launch thereby preventing propellant flow.	A) None

A) - Launch Conditions
B) - Flight

TABLE I-1 FAILURE EFFECT ANALYSIS MODEL ENGINE (SAMPLE) (Cont.)

Item	**	Drawing Number	Elect. Ref. Desig.	Function	Failure Type	Failure Effect on Subsystem Performance	Failure Effect on Stage	Failure Effect on Vehicle
2. (Cont.)							B) POSSIBLE LOSS OF STAGE: The pressure surge caused by the accumulation of a critical quantity of propellants may detrimentally affect the stage.	B) POSSIBLE LOSS
					b) Start	POSSIBLE LOSS OF ENGINE: If the valve opens prematurely enough to permit a critical quantity accumulation of propellants, a destructive pressure surge may occur during the igniter transient, otherwise the engine will start normally.	A) None B) POSSIBLE LOSS OF STAGE:	A) None B) POSSIBLE LOSS
					c) Operation	None: The valve is normally open during this phase of operation.	A) None B) None	A) None B) None
					d) Shutdown	Engine will continue running. However, shutdown can be accomplished by closing the tank safety valve (U4)	A) None B) None	A) None B) None

A) - Launch Conditions
B) - Flight

grouped together under a common heading. These headings are called "failure areas" or m's. A rough level is then defined for the failure tree; this level being referred to as the "failure defining level".

I-3. FAILURE CHARACTERISTICS

To be of maximum usefulness, the READI model engine must have failure characteristics which parallel those of real engines. This means that both the magnitude of failure probabilities and the distribution with respect to major components be representative of near future engines. All of the available failure data for current production and developmental engines were, therefore, collected and compared.

There is surprisingly good agreement in major subsystem failure rates from different sources, as can be noted in table I-2 where five different data sources are compared. The "used in analysis" column is not the average of high and low limits because consideration had to be given to the difference between the data source engines and the representative engine configuration.

The component failure rates were all normalized to give an engine which has a failure rate of 0.01 per run, or a reliability of 0.99. This means that the engine would fall into one of the four previously defined failure categories in one out of 100 firings. This figure is consistent with the current state-of-the-art for engines which have undergone extensive development effort.

A more detailed chart, which is divided by major malfunction areas, m's, is shown in table H-2. This chart shows the breakdown of assigned failure probabilities by m and by engine operating phase (prestart, start, etc.).

One condition which is troublesome from the standpoint of statistical independence is combustion instability. Combustion instability is really a failure effect, not a primary failure. However, the cause in each instance of combustion instability is difficult to trace and measure in real engines. Therefore, most analyses of rocket engines list instability as an independent failure and, therefore, it is listed in that way for the model engine.

I-4. LOSSES DUE TO FAILURES

The net worth of a READI system depends heavily on the stage design, the mission, and on crew safety criteria. Appendix F describes the evaluation procedure in detail. Figure I-2 shows the losses which must be generated for each malfunction for use in the mission loss evaluation.

TABLE I-2

FAILURE PROBABILITY DATA BY MAJOR SUBSYSTEM

Major Subsystem	Low Limit of Data		Hi Limit of Data		Used in Evaluation Procedure	
	% of Total Engine Failures	Failure Rate	% of Total Engine Failures	Failure Rate	%	λ
Turbopump Assembly	22	0.0022*	32	0.0052	22	0.0022
Thrust Chamber	14	0.0014*	32	0.0065	28	0.0028
Gas Generator	10	0.0016	17.1	0.00171*	12	0.0012
Valves	5.7	0.0014	31.7	0.00317*	24	0.0024
Line (Large and Small)	4.5	0.00045*	21	0.0034	9	0.0009
Regulators	-	0.0002	13.2	0.0030	3	0.0003
Starting System	1.9	0.00038	3.6	0.00036*	2	0.0002
Total for Engine					100%	0.0100

All failure rates are based on per cycle or per firing data

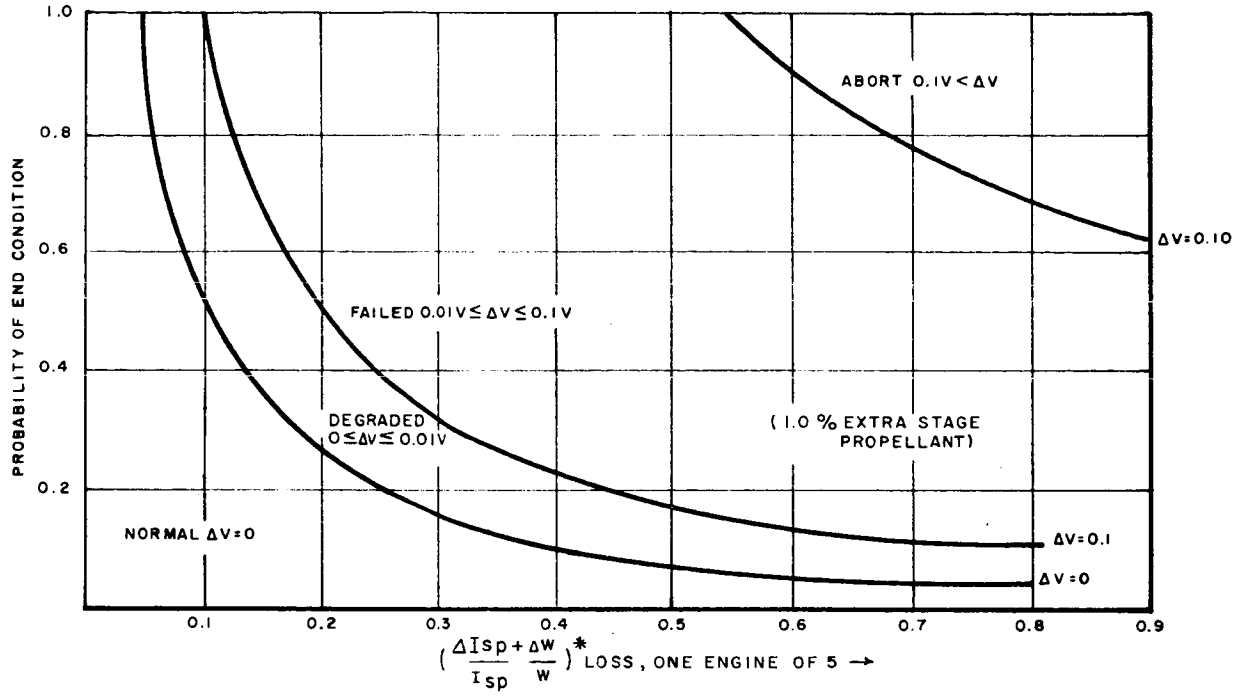
*Normalized total engine failure rate of 0.01

The engine loss data inputs are reduced to:

- loss of thrust
- loss of specific impulse from nominal
- loss of propellant overboard
- probability of explosion.

The losses have been calculated and/or estimated for all malfunction areas and engine phases, for all of the sets of programmed decisions, systems A through K, described in Appendix H. Table I-3 shows the losses for no READI and for one of the possible sets of READI programmed decisions, system H. The READI losses are divided into two categories of "loss with correct action" and "loss with false alarm". The loss with missed alarm is the same as no READI. System H has the ability to shutdown (normal and fast), restart, and increase thrust by 20 percent.

Losses of thrust, specific impulse and overboard propellant, resulting from failures which occur during the pre-start and start phases of the engine, carry through the whole operating phase of the engine, without corrective action. Failures during the operate phase are assumed to occur randomly. The resulting effect on the stage, i.e., normal, degraded, failed, and aborted, are then expressed in terms of the fraction of the stages ending up in the state for a given magnitude of the failure. Figure I-3 shows the fractional breakdown, i.e., normal, degraded, etc., for losses of specific impulse, overboard flow and thrust. Since the analysis has been performed for a second stage which normally does not require restart, the above losses have no effect during shutdown.



* OFF – DESIGN ENGINE OPERATION EFFECT PLUS OVERBOARD PROPELLANT EFFECT

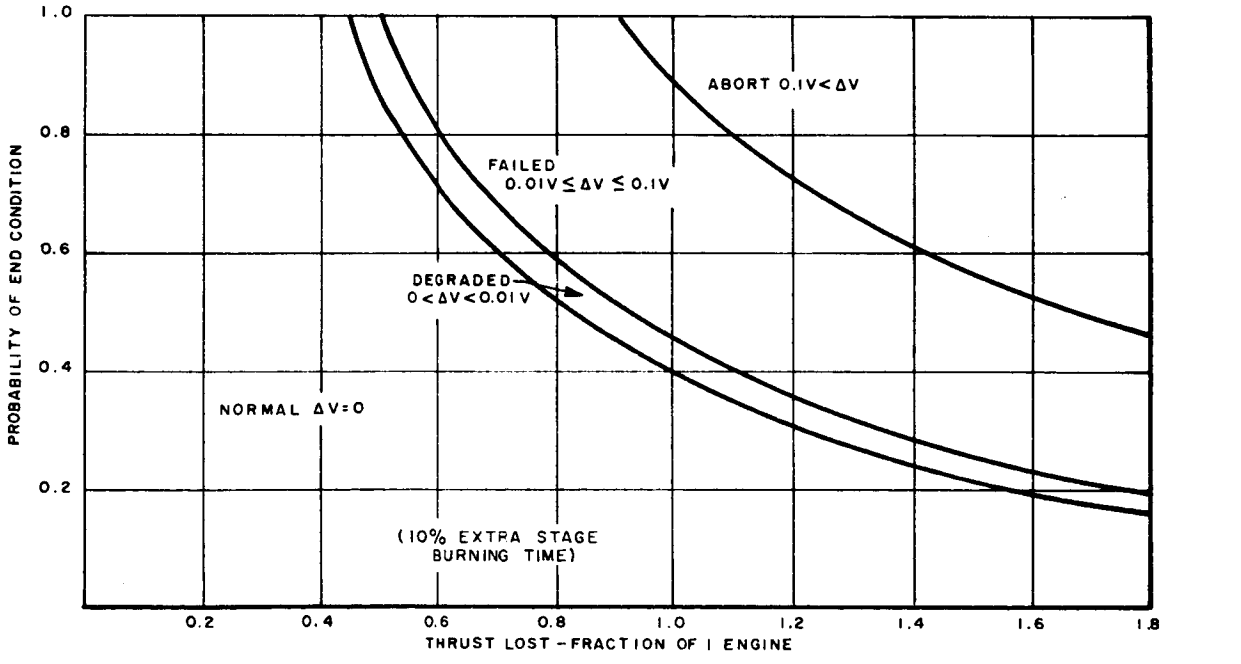


FIGURE I – 3 RELATIONSHIP BETWEEN PROPULSION SYSTEM LOSSES AND STAGE END STATES (FOR RANDOM OCCURRENCE DURING BURNING TIME)

TABLE I-3 PERCENT LOSSES WITH AND WITHOUT READI

		READI Inoperative or Missed Alarm				READI Operating Correctly				READI False Alarm For Decision Pattern H			
Malf. Area	Eng. Phase	Stage Thrust	Overboard Prop. Flow (One Engine)	I_{SP} (One Engine)	Expl. Prob.	Stage Thrust	Overboard Prop. Flow (One Engine)	I_{SP} (One Eng.)	Expl. Prob.	Stage Thrust	Overboard Prop. Flow (One Engine)	I_{SP} (One Engine)	Expl. Prob.
1 (Stage Failure)	1	100	0	0	0	100	0	0	0	100	0	0	0
	2	100	0	0	1	100	0	0	0	100	0	0	0
	3	100	0	0	1	100	0	0	0	100	0	0	0
	4	100	0	0	0	100	0	0	0	100	0	0	0
	5	100	0	0	1	100	0	0	0	100	0	0	0
2	1	-	-	-	-	-	-	-	-	-	-	-	-
	2	-	-	-	-	-	-	-	-	-	-	-	-
	3	1.8	3	4.0	50	4	0	0	0	4	0	0	0
	4	-	-	-	-	-	-	-	-	-	-	-	-
	5	-	-	-	-	-	-	-	-	-	-	-	-
3	1	-	-	-	-	-	-	-	-	-	-	-	-
	2	-	-	-	-	-	-	-	-	-	-	-	-
	3	3.8	17	(-) 2	50	4	0	0	0	4	0	0	0
	4	-	-	-	-	-	-	-	-	-	-	-	-
	5	-	-	-	-	-	-	-	-	-	-	-	-
4	1	-	-	-	-	-	-	-	-	-	-	-	-
	2	20	0	0	50	4	0	0	0	4	0	0	0
	3	20	0	0	50	4	0	0	0	4	0	0	0
	4	-	-	-	-	-	-	-	-	-	-	-	-
	5	20	0	0	50	4	0	0	0	4	0	0	0
5	1	-	-	-	-	-	-	-	-	-	-	-	-
	2	20	0	0	50	4	0	0	0	4	0	0	0
	3	20	0	0	50	4	0	0	0	4	0	0	0
	4	-	-	-	-	-	-	-	-	-	-	-	-
	5	20	0	0	50	4	0	0	0	0	0	0	0
6	1	-	-	-	-	-	-	-	-	-	-	-	-
	2	-	-	-	-	-	-	-	-	-	-	-	-
	3	4	0	0	0	4	0	0	0	4	0	0	0
	4	-	-	-	-	-	-	-	-	-	-	-	-
	5	-	-	-	-	-	-	-	-	-	-	-	-
7	1	-	-	-	-	-	-	-	-	-	-	-	-
	2	20	0	0	50	4	0	0	0	4	0	0	0
	3	20	0	0	50	4	0	0	0	4	0	0	0
	4	-	-	-	-	-	-	-	-	-	-	-	-
	5	20	0	0	50	4	0	0	0	4	0	0	0
8	1	100	0	0	99	4	0	0	0	4	0	0	0
	2	-	-	-	-	-	-	-	-	-	-	-	-
	3	-	-	-	-	-	-	-	-	-	-	-	-
	4	100	0	0	10	4	0	0	0	4	0	0	0
	5	-	-	-	-	-	-	-	-	-	-	-	-
9 (Stage Failure)	1	100	0	0	0	100	0	0	0	100	0	0	0
	2	100	0	0	1	100	0	0	0	100	0	0	0
	3	100	0	0	1	100	0	0	0	100	0	0	0
	4	100	0	0	0	100	0	0	0	100	0	0	0
	5	100	0	0	1	100	0	0	0	100	0	0	0
10	1	100	0	0	0	4	0	0	0	4	0	0	0
	2	20	0	0	50	4	0	0	0	4	0	0	0
	3	20	0	0	50	4	0	0	0	4	0	0	0
	4	100	0	0	0	4	0	0	0	4	0	0	0
	5	20	0	0	50	4	0	0	0	4	0	0	0
11	1	100	0	0	90	4	0	0	0	4	0	0	0
	2	-	-	-	-	-	-	-	-	-	-	-	-
	3	-	-	-	-	-	-	-	-	-	-	-	-
	4	100	0	0	9	4	0	0	0	4	0	0	0
	5	-	-	-	-	-	-	-	-	-	-	-	-
12	1	-	-	-	-	-	-	-	-	-	-	-	-
	2	20	0	0	10	4	0	0	0	4	0	0	0
	3	20	0	0	10	4	0	0	0	4	0	0	0
	4	-	-	-	-	-	-	-	-	-	-	-	-
	5	20	0	0	10	4	0	0	0	4	0	0	0
13	1	100	30	0	99	4	0	0	0	4	0	0	0
	2	20	30	0	90	0	0	0	1	0	0	0	0
	3	-	-	-	-	-	-	-	-	-	-	-	-
	4	100	30	0	54	4	0	0	0	4	0	0	0
	5	20	30	0	90	0	0	0	1	0	0	0	0
14	1	100	0	0	50	4	0	0	0	4	0	0	0
	2	-	-	-	-	-	-	-	-	-	-	-	-
	3	-	-	-	-	-	-	-	-	-	-	-	-
	4	-	-	-	-	-	-	-	-	-	-	-	-
	5	-	-	-	-	-	-	-	-	-	-	-	-
15	1	20	0	0	0	4	0	0	0	4	0	0	0
	2	20	0	0	10	4	0	0	0	4	0	0	0
	3	20	0	0	10	4	0	0	0	4	0	0	0
	4	20	0	0	0	4	0	0	0	4	0	0	0
	5	20	0	0	10	4	0	0	0	4	0	0	0
16	1	-	-	-	-	-	-	-	-	-	-	-	-
	2	20	20	0	99	4	0	0	3	4	0	0	0
	3	20	20	0	99	4	0	0	3	4	0	0	0
	4	-	-	-	-	-	-	-	-	-	-	-	-
	5	20	0	0	99	4	0	0	3	4	0	0	0
17	1	-	-	-	-	-	-	-	-	-	-	-	-
	2	-	-	-	-	-	-	-	-	-	-	-	-
	3	(-) 1.2	3	(-) 1.7	10	4	0	0	0	4	0	0	0
	4	-	-	-	-	-	-	-	-	-	-	-	-
	5	-	-	-	-	-	-	-	-	-	-	-	-
18	1	-	-	-	-	-	-	-	-	-	-	-	-
	2	-	-	-	-	-	-	-	-	-	-	-	-
	3	(-) 3.2	17	3.1	10	4	0	0	0	4	0	0	0
	4	-	-	-	-	-	-	-	-	-	-	-	-
	5	-	-	-	-	-	-	-	-	-	-	-	-
19 (Stage Failure)	1	-	-	-	-	-	-	-	-	-	-	-	-
	2	-	-	-	-	-	-	-	-	-	-	-	-
	3	0	2	0	0	(-) 20	2	0	0	(-) 20	0	0	0
	4	-	-	-	-	-	-	-	-	-	-	-	-
	5	-	-	-	-	-	-	-	-	-	-	-	-
20	1	0	0	0	50	0	0	0	1	0	0	0	0
	2	0	0	0	50	4	0	0	1	4	0	0	0
	3	50	0	0	50	4	0	0	1	4	0	0	0
	4	0	0	0	50	0	0	0	1	0	0	0	0
	5	0	0	0	50	4	0	0	1	4	0	0	0
21	1	-	-	-	-	-	-	-	-	-	-	-	-
	2	0	0	0	10	4	0	0	0	4	0	0	0
	3	0	0	0	10	4	0	0	0	4	0	0	0
	4	-	-	-	-	-	-	-	-	-	-	-	-
	5	0	0	0	10	4	0	0	0	4	0	0	0
22 (Stage Failure)	1	-	-	-	-	-	-	-	-	-	-	-	-
	2	-	-	-	-	-	-	-	-	-	-	-	-
	3	0	8	0	0	(-) 20	8	0	0	(-) 20	0	0	0
	4	-	-	-	-	-	-	-	-	-	-	-	-
	5	-	-	-	-	-	-	-	-	-	-	-	-
23	1	-	-	-	-	-	-	-	-	-	-	-	-
	2	-	-	-	-	-	-	-	-	-	-	-	-
	3	20	0	0	60	4	0	0	0	4	0	0	0
	4	20	0	0	0	4	0	0	0	4	0	0	0
	5	-	-	-	-	-	-	-	-	-	-	-	-
24	1	0	0	0	0	4	0	0	0	4	0	0	0
	2	0	0	0	0	4	0	0	0	4	0	0	0
	3	50	10	5	10	4	0	0	0	4	0	0	0
	4	0	0	0	0	4	0	0	0	4	0	0	0
	5	0	0	0	0	4	0	0	0	4	0	0	0
25	1	0	0	0	0	4	0	0	0	4	0	0	0
	2	0	0	0	90	4	0	0	0	4	0	0	0
	3	0	0	0	90	4	0	0	0	4	0	0	0
	4	0	0	0	0	4	0	0	0	4	0	0	0
	5	0	0	0	0	4	0	0	0	4	0	0	0

NOTE: Losses Are Expressed As:

1 - Stage Thrust - Percent Loss from 5 Engine Thrust

2 - Overboard Prop Flow - Percent of Single Engine Flow at 100% Thrust

3 - I_{SP} - Percent Loss of Specific Impulse from Nominal, 420 sec.

4 - Explosion (one engine) Probability - Percent Probability of Explosion, Given The Malfunction, m (one engine)

Appendix J
ENGINE OVERRATING

APPENDIX J

ENGINE OVERRATING

J-1. INTRODUCTION

Repeated reference is made throughout this report to the use of engine-out capability to achieve the prime mission when it is necessary to shut down one engine in a cluster. This capability may be achieved by planning the mission so that the objectives may be achieved by running the remaining engines for a longer time, or by overrating the remaining engines in case of a shutdown, or a combination of these techniques. Rocketdyne has investigated the extra burning time approach; this appendix examines briefly the problem of overrating.

J-2. SUMMARY

The stress environment was investigated for several major turbopump subcomponents, namely the pump discharge volute case, turbine wheel, and turbine manifolding. The phenomenon of pump cavitation was examined for two different conditions of design, total inlet pressure, or net positive suction head. Results are shown as the component failure rate as a function of operating level, given in terms of percent full-thrust of the rocket engine.

Figure J-1 shows a non-linear increase in percent failure rate of components of a rocket engine as thrust is increased above the design point. The pump cavitation curve B, for instance, shows that the pump cavitation rate is about 7 percent at 120 percent thrust. Stated differently, the pump will cavitate in 7 out of 100 starts. Analysis of rocket engine test data indicates that at normal thrust a cryogenic pump might cavitate in one out of 200 starts with the normal variation in pump inlet conditions. The failure rate has then gone up by a factor of 14. Other components show a higher increase in failure rate while some are unaffected at 120 percent thrust.

The overrating action would always be programmed into the operate phase of the engine. The engines would therefore proceed through a normal start and then be increased 20 percent in thrust. Only selected components in the READI model engine are effected by overrating. If, for instance, the maximum failure rate increase of the

most critical component was 100 percent, the model engine undergoes a 75-percent increase in overall failure rate in the operate phase. The following table summarizes this hypothetical situation after shutdown of one engine.

Engine Phase	Stage Failure Rate = 4 x Engine Failure Rate	
	Without Overrating	With 20% Overrating
Prestart + Start	0.0158	0.0158
Operate	0.0236	0.0412
Shutdown	0.0016	0.0016

As the component failure rates are allowed to increase by a greater factor with overrating the idea becomes less attractive. A trade-off must therefore be made among the following:

- percent increase in thrust
- increase in component failure rates
- possible redesign of critical parts
- extra burning time margin and resulting payload penalty.

The last item enters the picture because a combination of overrating and extra burning time is a likely compromise. Figure J-3 shows the trade-off between extra burning time and degree of overrating for a five-engine cluster.

J-3. ANALYTICAL PROCEDURE

The ability of a system to satisfy design objectives for a desired period of time is a probabilistic phenomenon. In each of the system components, there are variations in operating characteristics and environments with associated variations in the stress distribution throughout each component. Similarly, there are variations in the strength of each component. Failure occurs, by definition, when the stress exceeds the available strength. Generally, the probability of failure of a system, taken as the sum of the failure probabilities of each of the system components, follows a normal distribution defined by a mean, μ, and standard deviation, σ, (reference 1).

When the desired operating characteristics for a system are established, a general design procedure is as follows:

a. Estimation of the variation in each component's operating characteristics, based on past experience. Variations in operating characteristics are given in terms of the

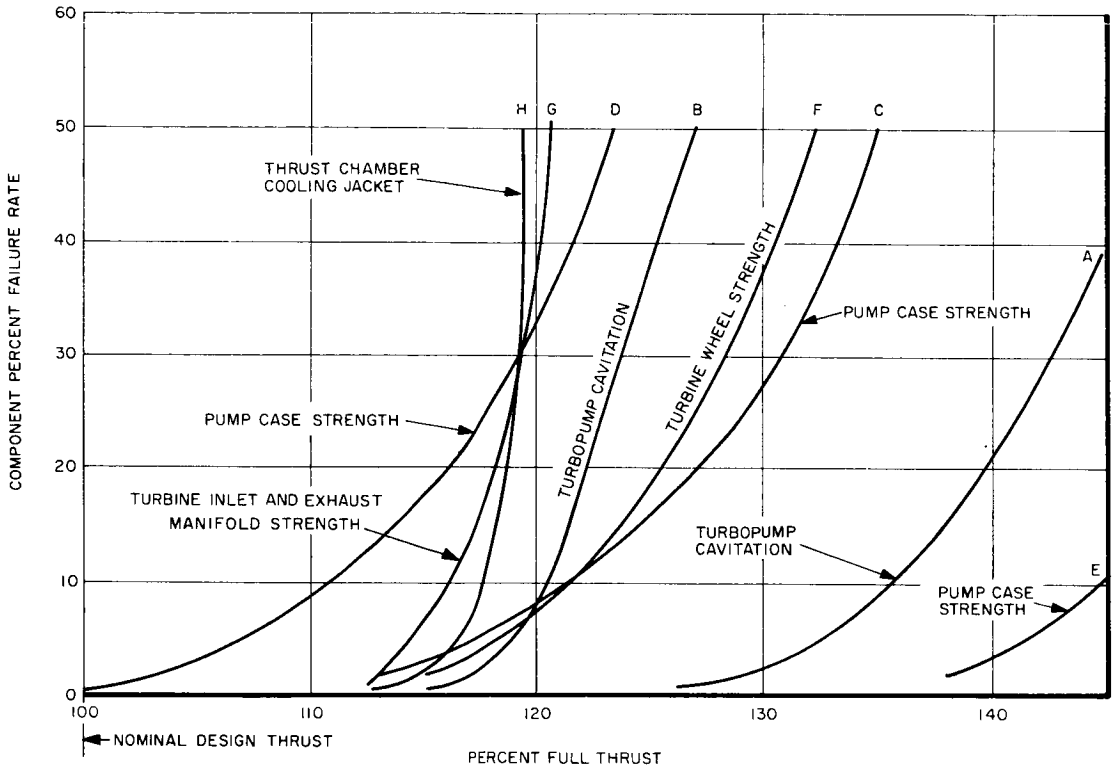


FIGURE J-1

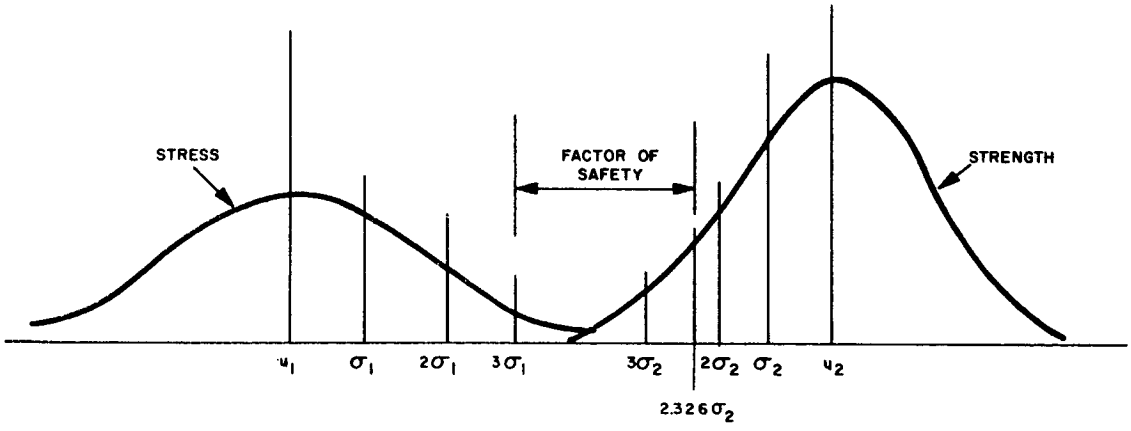
TYPICAL COMPONENT FAILURE RATES
VS ENGINE THRUST

standard deviation of the normal distribution, and the coefficient of variation, defined as the standard deviation divided by the mean. (Typical coefficients of variation for rocket engine components generally range between 0.03 and 0.08.)

b. Calculation of the maximum expected stress level in terms of component physical characteristics. The maximum expected stress level is defined as that corresponding to the maximum expected environment to three standard deviations. When multiplied by the desired factor of safety, this becomes the minimum allowable strength.

c. Determination of the available allowable strength, and comparison with the required minimum allowable strength from step b, for solution of required physical characteristics. (The minimum allowable strength is usually defined as the strength that 99 percent of the material will exceed, reference 2, which corresponds to 2.326 standard deviations.)

This procedure may be illustrated as follows:



Note that there is some overlapping of the stress and strength distributions; it is this overlapping area that defines the failures; i.e., where the stress exceeds the strength. The overlapping area depends on the standard deviations of the stress and strength distributions, and the factor of safety. The probability of failure is the value of the overlapping area compared to one, which is the total area under each normal curve.

For a given design, then, the effect on failure probability for operating levels exceeding the design value may be found by calculating the overlapping area when the mean of the stress curve is moved toward the strength curve.

The following symbols are used:

	Stress (or environment)	Strength (or resistance)
Normal Distribution	y_1	y_2
Mean	x_1	x_2
Standard Deviation	σ_1	σ_2

The equations of the two curves are

$$y_1 = \frac{N}{\sigma_1\sqrt{2\pi}}\, e^{-\frac{1}{2}\left(\frac{x - x_1}{\sigma_1}\right)^2} \quad \text{and} \quad y_2 = \frac{N}{\sigma_2\sqrt{2\pi}}\, e^{-\frac{1}{2}\left(\frac{x_2 - x}{\sigma_2}\right)^2}$$

Equating and solving for x,

$$x = \left(\frac{x_1}{\sigma_1^2} - \frac{x_2}{\sigma_2^2}\right) \pm \sqrt{\left(\frac{x_1}{\sigma_1^2} - \frac{x_2}{\sigma_2^2}\right)^2 + \left[\frac{2\ln\frac{\sigma_1}{\sigma_2} + \frac{x_1^2}{\sigma_1^2} - \frac{x_2^2}{\sigma_2^2}}{\left[\frac{1}{\sigma_2^2} - \frac{1}{\sigma_1^2}\right]}\right]}$$

Using the value of x and the values of the standard deviations, the overlapping areas may be calculated with the aid of a table of areas of the normal curve (for example, reference 1).

It can be seen that x_1 corresponds to the mean stress value for 100 percent of design load. For higher values, x_1 is multiplied by an appropriate factor (1.05 for 105 percent, etc.) and a new value of x and a new overlapping area computed. In this way, a curve of probability of failure as a function of design load can be constructed for a particular component and a given set of parameters. Figure J-2 shows an example of such a calculation for the example of pump cavitation. Overall rocket engine system probability of failure, P_f, can then be found as the sum of all the component failure probabilities, P_{fn}. For low overall system failure probabilities

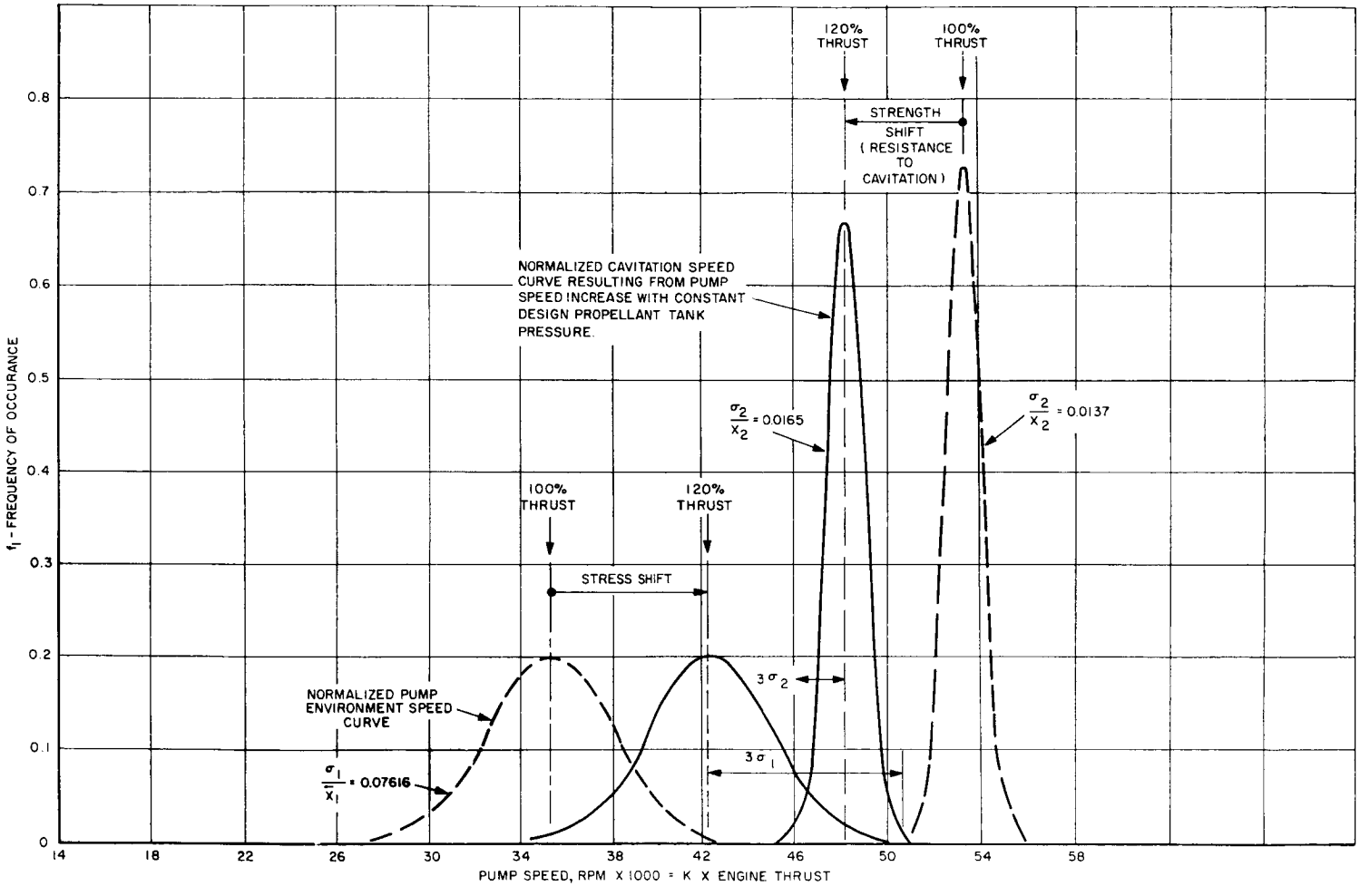


FIGURE J-2

EFFECT ON PUMP CAVITATION
OF INCREASE IN ENGINE THRUST

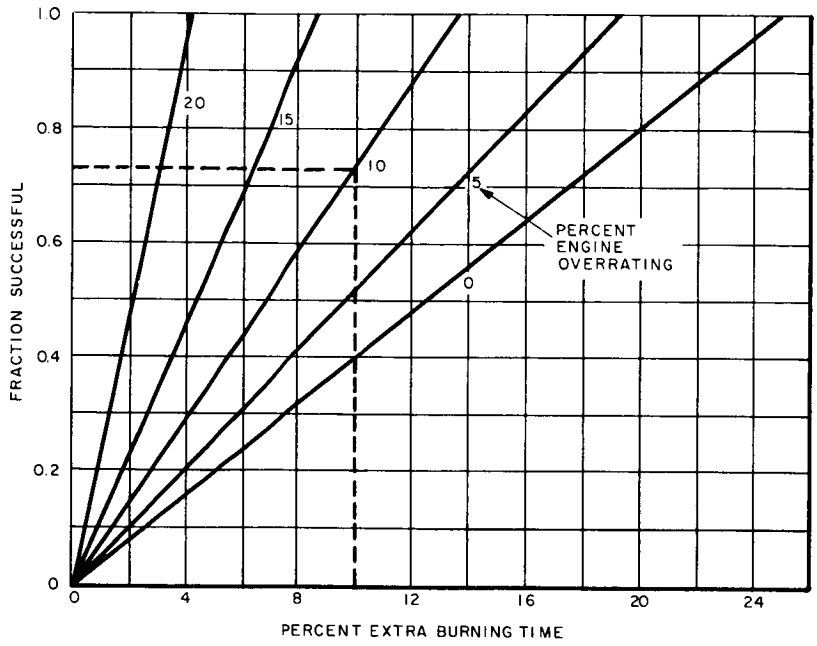


FIGURE J-3, ATTAINMENT OF DESIGN TERMINAL VELOCITY AFTER SHUTDOWN OF 1 OF 5 ENGINES (FOR RANDOM OCCURRENCE DURING BURNING TIME)

$$P_f = P_{f_1} + P_{f_2} + P_{f_3} + \ldots + P_{f_n} \quad \text{(less than 1\% error for } P_f < 0.02\text{)}$$

or more generally,

$$P_f = 1 - (1 - P_{f_1})(1 - P_{f_2})(1 - P_{f_3}) \ldots (1 - P_{f_n})$$

In this manner, the rate of change of probability of failure with changing parameters can be determined, and a particular probability curve for a given configuration found. As previously noted, coefficients of variation for rocket engine components generally range from 0.03 to 0.08; for most commonly used materials, the coefficient varies from 0.015 to 0.05 (references 3 and 4). Factors of safety range from 1.0 to 2.0, depending on the particular application and specification. A typical set of parameters used in the calculations is:

Coefficient of variation for pressurized components: 0.060

Coefficient of variation for turbopumps: 0.075

Coefficient of variation for 2014-T6 aluminum alloy: 0.032

Safety factor for typical booster engine: 1.5

J-4. TURBOPUMP ANALYSIS

This method of analysis has been utilized to conduct a study of turbopump failure rates when the engine is operated above design thrust. Insight to the failure probability of the turbopump, as well as other engine components, will help define the engine overrating capability and also suggest areas where improvements in reliability can be made. It should be appreciated that the resulting data is not necessarily indicative of all turbopump designs since in many cases the design safety factors are tempered by the individual designers and can vary considerably. Manufacturing considerations also have an important influence on designs. Therefore, to obtain an accurate evaluation of the operational probability of failure on turbopumps, or any component, it is necessary to evaluate the individual component in detail and work with the actual design safety factors.

J-5. PUMP VOLUTE, TURBINE WHEEL, AND TURBINE MANIFOLD

Operational failure can occur either of two ways: namely, stress and performance. Each condition will have an operational environment probability and resistance to fail probability. A pump case, for example, will be subjected to a pressure which will exert a

stress on the walls. However, because of the operational tolerances of the overall system, where the pump is only one component, the pump pressure will vary. At the same time, the pump case walls will experience a stress vibration which will be proportional to the pressure.

These variations can be determined from limited testing, and by applying statistical methods of analysis, a probability of occurrence curve can be obtained. In this case, the curve would represent the environment of the pump case stress. In order to complete the analysis of operational failure, it becomes necessary to determine the stress resistance probability curve. This is required since the pump case material is subjected to strength tolerances due to manufacturing processes such as heat treatment, etc. Also, the pump case wall thickness will vary due to manufacturing tolerances which will affect the strength or resistance to fail.

In case of operational failure of performance, the same approach to solving probability of failure is taken. However, quite often the resistance to failure probability curve will shift simultaneously with the environmental probability curve causing a rapid convergence towards 100-percent failure probability. (Actually, this condition can exist in a stress failure analysis if the strength of the material is permitted to deteriorate, possibly due to temperature or radiation.)

The stress environment was investigated for several major turbopump subcomponents consisting of pump discharge volute case, turbine wheel, and turbine manifolding. (There are many other subcomponents in a turbopump which would require analyzing but the effort involved for this report would be prohibitive. Examples of these subcomponents are seals, bearings, impellers, gearing, and shafting.) As the turbopump output (flow) is increased through a speed increase, which is essentially proportional to engine thrust, pressures in the pump cases and turbine manifolds increase. Likewise, the centrifugal stresses in the turbine wheel increase as the speed increases. In each case, the stress can be related to the pump speed parameter. The pump case pressure (or stress) and the turbine wheel stress vary directly as the square of the speed. The turbine manifold pressure (or stress), however, varies directly as the cube of the speed if pump horsepower (pressure x flow) is to be satisfied by increasing the turbine drive gas flow rate while maintaining constant temperature. Increasing the gas flow rate through constant flow areas will require a rise in gas pressure which follows the cubic relationship with speed. In all the above relationships with speed, the assumption is made that

the efficiencies of the pumps and turbine, and the thrust chamber performance remain essentially constant. This is a valid and necessary assumption for this broad analysis.

Several conditions of failure probability related to stress were investigated for the pump cases and are depicted in figure J-1C, D and E. In some designs, practical manufacturing considerations will result in a design which will have a very large factor of safety, and hence a small failure probability. This is often experienced in a small pump where the wall thickness is "beefed-up" to attain a practical value that is consistent with accepted casting techniques. A stress check might reveal this design to have a tremendous factor of safety.

Figure J-1C is typical for the LR99 pump case where a 1.5 factor of safety plus a transient factor were used in the design and called out in MIL-E-5150 specification. During manufacturing of the pump cases, a proof pressure check corresponding to the design safety factor is made to determine the vaidity of the design. (A similar test is also made with the turbine wheel by spin tests with a temperature gradient corresponding to design temperature conditions.)

J-6. CAVITATION

In the cavitation failure probability analysis, two conditions were evaluated. Before explaining these conditions, it would be helpful to understand the cavitation phenomenon and how it affects pump performance. Basically, cavitation occurs when the local static fluid pressure reaches the vapor pressure. (In a pump, this condition begins to occur on the leading edges of an impeller at the maximum radius where the relative velocity is a maximum. Under violent cavitation, vapor bubbles will form and then collapse under the higher upstream pressures. This action causes erratic pump flow and then complete loss of flow.) During normal operating conditions, the local static pressure is always greater than the fluid vapor pressure. However, the relative velocity can be increased to a point where the local fluid static pressure (according to Bernoulli's theory) will decrease and equal the fluid vapor pressure where cavitation will commence. This is the phenomenon which occurs when a pump is run above its design point. Both the fluid velocity and blade velocity increase tend to reduce the local static pressure.

Two cavitation failure probability analyses were performed. The first assumed that the design total inlet pressure or net positive suction head (NPSH) was always available as the pump demand was increased. This is depicted in figure J-1A and implies that the inlet

pressure line losses, due to increased flow, are made up by increasing the line size or increasing the propellant tank pressure. In this analysis, the cavitation resistance curve remains fixed as the environment curve begins to shift. (The probability cavitation resistance curve was determined from the X-15 propellant tank pressure regulator tolerances.) The second cavitation failure probability analysis assumed that the design propellant tank pressure was held constant as the pump demand was increased. In this condition, as the pump was uprated, both the environment and resistance curves closed in on one another (figure J-2) which resulted in the cavitation failure probability curve in figure J-1B. Figure J-2 was generated considering PFRT test data, which was used to obtain an idea of the spreading of the distribution curves.

In conclusion, it should be mentioned that there is a practical limit in uprated turbopumps. Although pump affinity laws indicate no limit with respect to flow (cavitation disregarded), each pump design has its own particular limit which must be determined experimentally. The factor which limits the pump output is the frictional loss which increases at a greater rate than the developed head output rate. In general, pumps can run safely with flow increases up to 25 percent if sufficient NPSH is available.

J-7. THRUST CHAMBER ANALYSIS

A variation of the method of analysis used on the turbopump was used to determine the failure probability associated with uprating the thrust chamber of an engine. An 80,000 pound thrust, Thiokol-RMD designed hydrogen-oxygen engine was selected for an example. This unit is regeneratively cooled to an area ratio of 17:1. Chamber pressure and O/F ratio were 600 psia and 5, respectively. A single stage igniter also formed part of the thrust chamber design. The failure mode examined is a pressure-induced failure of the chamber cooling tubes resulting from loss of material strength at elevated temperature.

The following parameters were evaluated as a function of variable chamber pressure for valves of 600 psia and up.

- Gas side-wall temperature in the throat
- Mean wall temperature in the throat
- Pressure drop from cooling jacket inlet to combustion chamber (igniter throat conditions were not evaluated since the mass velocity is relatively low due to the subcritical pressure ratio from the igniter to main combustion chambers).

A typical tolerance of heat transfer rates from assembly-to-assembly of a developed design is about ± 5 percent of the nominal. For the purposes of this analysis, the nominal value was defined as the design calculation value for the 80,000 pound unit. Similarly, thrust chamber cooling jacket pressure drop variations from assembly-to-assembly of a developed design are typically ± 8 percent. The above tolerances were applied to determine maximum and minimum parameter values at each nominal chamber pressure level considered.

Gaussian distributions were assumed to exist between the above limits which were taken to be 3 sigma levels. Thus, the one-sigma variations were ± 1.7 and ± 2.7 percent respectively for heat transfer rates and cooling jacket pressure drop. The following list tabulates the pertinent parameters of interest for the 80,000 pound design at the nominal chamber pressure condition of 600 psia.

Gas side-wall temperature at throat = 1000°F

Mean wall temperature at throat = 904°F

(0.010 thick "D" or "E" nickel)

Inlet pressure to cooling jacket = 939 psia

Pressure drop from inlet to cooling jacket to combustion chamber = 339 psi

Gas side-wall temperature does not increase very rapidly with thrust level because of the very small temperature drop through the 0.010-inch thick nickel tube walls.

Figure J-1H shows a typical failure probability curve that can be generated for an assumed maximum allowable jacket inlet pressure of 1200 psia.

REFERENCES FOR APPENDIX J

1. Applied General Statistics by F. Croxton and I. Cowden, Prentice-Hall, Inc., 1955

2. MIL-HDBK-5, March 1961

3. "The Fundamental Aspects of Structural Reliability" by I. Bouton, IAS Paper No. 62-32, Annual Meeting January 1962, Inst. of Aerospace Sciences.

4. "Predicting Performance Failures" by G. Cohen, Machine Design, October 3, 1957.

REFERENCE DATA FOR FIGURE J-1

Figure J-1A: Turbopump Cavitation Percent Failure Rate vs. Percent Engine Thrust

note: a) Design net positive suction head at pump inlet held constant

b) Based on LR99 turbopump

Figure J-1B: Turbopump Cavitation Percent Failure Rate vs. Percent Engine Thrust

note: a) Propellant tank design pressure held constant (net positive suction head at pump inlet decreasing due to inlet losses as flow is increased)

b) Based on LR99 turbopump

Figure J-1C: Pump Case Strength Percent Failure rate vs. Percent Engine Thrust

note: a) Based on minimum factor of safety for man-rated applications per MIL-E-5150.

b) Typical for critical sections on LR99 pump

c) Safety Factor = 1.5 x working pressure + pressure increase due to 10-percent overspeed. Therefore, proof pressure = $1.5\ P_W + \left[(1.1)^2 - 1\right] P_W = 1.71\ P_W$

Figure J-1D: Pump Case Strength Percent Failure Rate vs. Percent Engine Thrust

note: a) Based on Safety Factor = 1.25 x working pressure + pressure increase due to 10-percent overspeed or proof pressure = $1.46\ P_W$

Figure J-1E: Pump Case Strength Percent Failure Rate vs. Percent Engine Thrust

note: a) Based on pump case design dictated by manufacturing considerations typical for low thrust engines and similar to corvus pump (1000-lb thrust)

Figure J-1F: Turbine Wheel Strength Percent Failure Rate vs. Percent Engine Thrust

note: a) Based on minimum factor of safety for man-rated applications per MIL-E-5150.

b) Typical for critical sections on LR99 turbine.

c) Safety factor = 1.5 x working stress + stress increase due to 10-percent overspeed.

Figure J-1G: Turbine Inlet and Exhaust Manifold Strength Percent Failure Rate vs. Percent Engine Thrust

note: a) Based on minimum factor of safety for man-rated applications per MIL-E-5150.

b) Typical for critical sections on LR99 turbine

c) Safety factor = 1.5 x working stress + stress increase due to rise in manifold pressure to cause 10-percent overspeed.

Figure J-1H: Thrust Chamber Cooling Jacket Percent Failure Rate vs. Percent Engine Thrust.

note: a) Assumed maximum allowable jacket inlet pressure of 1200 psia.

Appendix K

TECHNIQUES OF ENGINE CONDITION IDENTIFICATION

APPENDIX K

TECHNIQUES OF ENGINE CONDITION IDENTIFICATION

K-1. INTRODUCTION

The function of the READI system is to make in-flight decisions based on the condition of the propulsion system.

A set of parameters can be selected that will completely describe the condition of the propulsion system. However, since the propulsion system is a very complex distributed physical system, to describe completely the state of operation for all normal and malfunction modes of operation would require a very large number of these parameters. But, if some engineering judgment is applied and only significant measurable parameters are used, the selection can be considerably reduced.

Any specific operating condition can be envisioned as a point in a multi-dimensional signal space of which each dimension is one of the measured variables. Sets of similar operating conditions can be thought of as contiguous points or volumes in this signal space and identified as particular malfunctions or as normal operation, as shown in figure K-1 for a two-dimensional system.

It is, of course, not necessary for the READI system to be able to determine the exact point in signal space that describes the engine condition. In fact, it is not even necessary to localize the condition to a particular malfunction. It is only necessary to localize the condition to a region for which, considering all factors, a particular decision is most appropriate. This region may encompass a number of specific malfunctions.

Separation of these regions can be made by sets of planes with the volumes on the two sides of the plane identified by binary 0 and 1. These signal space separations are indicated by lines on figure K-1 and the regions to each side of the separations are identified as V_j and $\overline{V}_j$. Using Boolean notation the resulting combination of regions can be identified as shown in the lower part of the illustration.

The design of signal space separations requires considerable ingenuity. Included in the design process are: selection

of an appropriate variable or set of variables, suitable transducers, signal transformation, and comparison with a stored reference.

The most valuable guide in the preliminary hypothesis of signal space separations is the failure effects tree shown in figure I-1. The investigator is free to range over the entire pattern or tree in search of suitable separations, since most separations may be accomplished in a variety of functionally redundant ways. Some considerations in the design of signal space separations are:

- The set of possible decisions which can be programmed
- The sensitivity of the measurements. It is desirable to choose measurements that are orthogonal to the desired plane of separation. This has the effect of reducing transducer accuracy requirements and tends to simplify signal processing
- The losses incurred from the failure. The seriousness of the final engine state can be measured in terms of loss of thrust, loss of propellant overboard, loss of specific implulse, and probability of explosion.
- The rate at which the failure propagates through the engines.

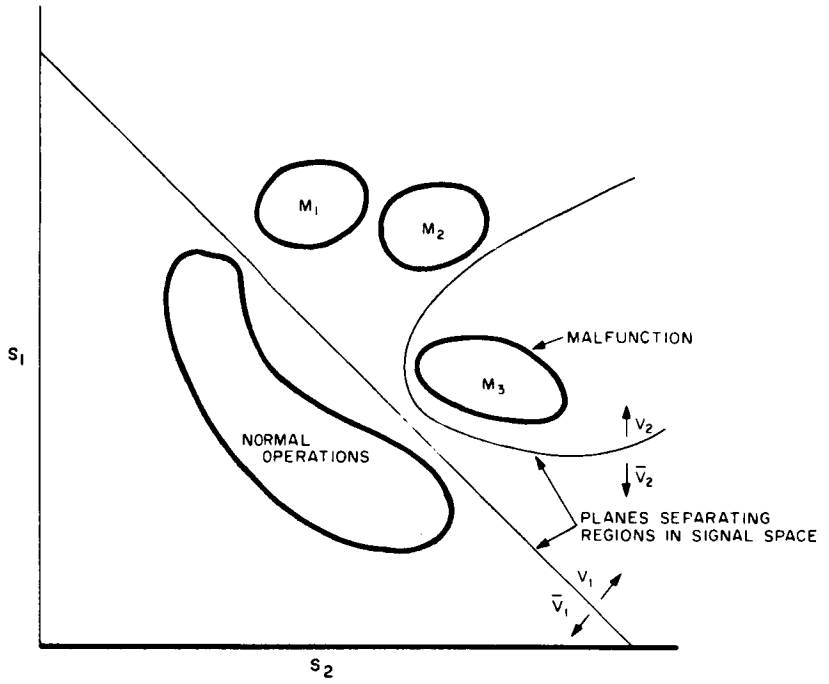
K-2. DESIGN OF SIGNAL SPACE SEPARATIONS

A. BOOLEAN FUNCTIONS

The simplest type of signal space separation involves the comparison of the magnitude of a signal to a fixed limit. For example, when a simple temperature sensitive fire detector indicates a temperature in excess of a limit around the turbine exhaust, a corrective action, shut down, is clearly indicated. If the condition is allowed to prevail, the entire stage may be destroyed.

Note that no other signal need be used, only the fire-detector signal and its reference. For convenience, when the temperature exceeds to limit, the signal, S, is set equal to binary one. The signal space separation, V, in this case, is simply V = S.

Generally, two or more input signals, S's, are required to effect the desired separation, V. For example, in the first sketch in figure K-2, when S_1 and S_2 exceed their respective limits, the V obtained is as shown in the shaded area. There is not theoretical limit



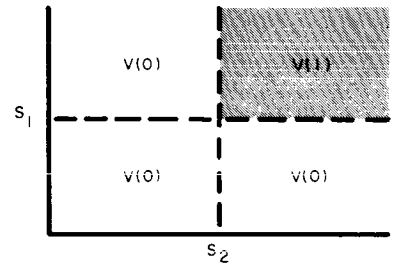
LEGEND

$\overline{V}_1$ REGION FOR NORMAL OPERATION
V_1 REGION CONTAINING ALL MALFUNCTIONS
V_2 REGION CONTAINING M_3
$V_1 \overline{V}_2$ REGION CONTAINING M_1 AND M_2

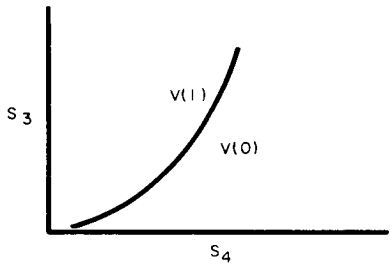
FIGURE K-I

SIGNAL SPACE DESCRIBING PROPULSION SYSTEM STATES
FOR NORMAL AND MALFUNCTION OPERATING CONDITIONS

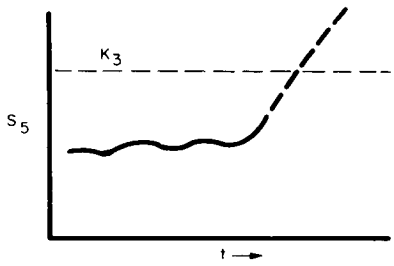
1. BOOLEAN FUNCTION
   OF n VARIABLES
   $V = S_1 S_2$



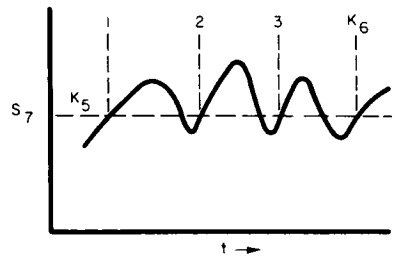
2 ARITHMETIC FUNCTION
   n VARIABLES
   $V = 1$ FOR $S_3 > K_1 (S_4)^2$



3. TIME FUNCTIONS OF
   n VARIABLES
   $V = 1$ FOR $S_5 + K_2 \frac{dS_5}{dt} > K_3$ OR
   $V = 1$ FOR $\int_0^t S_6 \, dt > K_4$



4 NUMBER OF EVENTS
   $V = 1$ FOR $\Sigma (S_7 > K_5) > K_6$



CODE
V = SIGNAL SPACE SEPARATION
S = SIGNAL
K = CONSTANT

FIGURE K-2
TYPES OF SIGNAL SPACE SEPARATIONS

to the number of S terms which may be "anded" together (and therefore to the dimensions of the sketch). In practice, however, the maximum number of "anded" terms used in the V equations for the READI model engine was three. A combination of S's will contain one "indicator" S and the rest will be "gate" S's.

A single input may be processed or quantized to a number of different levels for use in various equations. Turbine speed, for instance, is quantized to six different speed values in the complete list of signal space separations for the READI model engine.

B. ARITHMETIC FUNCTIONS

Effective separation of the engine signal space in many cases requires arithmetic operations on several variables. For instance, m3, low chamber oxygen flow, can be detected in part by the following:

$$5(S12) - S11 > 43 \text{ lb/sec}$$

This is, in essence, a statement of discrepancy in chamber propellant flow. The processed signal, 5(S12), "five times fuel flow", is nominally equal to S11, the oxygen flow.

In some cases it is necessary to resort to more involved calculations. For instance M17, high fuel flow to chamber, is detected by measuring mass flow at two stations on the engine and comparing the answers. The mass flow at the flowmeter, FM1, is compared to the mass flow computed from the injector pressure drop. Appendix E describes in detail how some of these measurements are made. Briefly, the turbine meter reading is corrected to indicate mass flow with fuel temperature and fuel pressure inputs.

$$W_p = k_1 Q_p (1 - k_2 \Delta T - k_3 \Delta P)$$

where

W_p = propellant mass flow

Q_p = propellant quantity flow

ΔT = deviation from nominal propellant temperature

ΔP = deviation from nominal propellant pressure

k's = constants.

The mass flow indication at the fuel injector is derived from pressure drop and temperature inputs. The final comparison can be made using either a straight line approximation to the parabolic flow curve or an exact equation. Since fuel flow can be used in a number of separations, the calculation is made once and used in several places.

C. ARBITRARY TIME FUNCTIONS

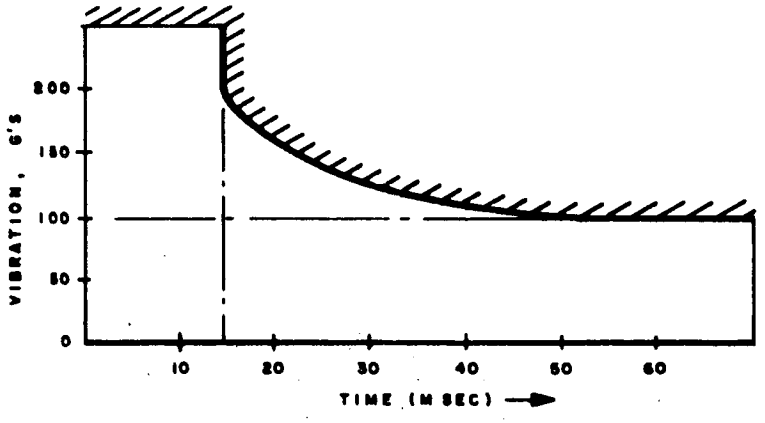
A signal may be differentiated or integrated to effect a desired separation. Figure K-2 curve number 3 shows a simple predictive time function. Many Boolean separations employ time "gates" to phase the separation properly in the engine operation cycle. In some cases limits are also time dependent. The time scale can vary considerably in magnitude. Examples are:

Very short - 0.050 seconds for combustion instability

Medium - 10 seconds for turbine burnout

Long - 200 seconds for minimum ullage pressure to maintain tank structural integrity.

The vibration limit, for instance, is shown in the accompanying sketch.



K-3. EXAMPLE OF DEVELOPMENT OF SIGNAL SPACE SEPARATION

Consider the failure, fuel pump cavitation, m4. It is desirable to isolate m4 and m5, oxidizer pump cavitation, from the other failures which cause propellant flow interruption, because a restart attempt is scheduled for m4 and m5 and not for the others.

One place to start in hypothesizing V equations is to examine normal starting transient curves; these are usually expressed in terms of propellant flows and pressures, and pump speed versus time. The starting transients are of particular interest because cavitation is more likely to occur at start, and there is an explosion hazard associated with undetected cavitation at start. The corresponding transients which occur during cavitation are measured from actual test, estimated from tests which produce similar effects as calculated. Figure K-6 shows a family of curves for pump speed, pump discharge pressure, and time.

When cavitation occurs, the pump discharge pressure falls below normal and the speed goes above normal, because the turbine has lost part of its load. Time can be eliminated to reduce the problem to two dimensions as shown in the bottom sketch (figure K-6) where percent speed is plotted versus percent pressure.

A possible V equation is therefore

$$V = 1 = (S6)\ (S33)$$

where the following definitions of binary one are used:

S6 > 90% speed

S33 < 60% pressure.

It is now necessary to examine this candidate V for validity under all failure conditions. Consider, for instance, the sudden closure of the tank safety valve (U4). Unfortunately, almost exactly the same signals result. Since a different decision is invoked for the U4 closed failure, the candidate V is unsatisfactory. The following two points give a clue to a suitable answer. Since the tank safety valve, U4, on the model engine is a linked valve, the failure of U4 will produce almost identical effects on the two pumps. On the other hand, it quite unlikely to cavitate both pumps due to insufficient priming, because this required simultaneous, independent failures in other parts of the engine. Therefore, if a new comparison, similar to that in figure K-6 is made between fuel and oxidizer pump discharge pressures, a more definitive separation can be made.

$$V = 1 = (S32)\ (S33)$$

where the following definitions of binary one are used:

S32 > 75% pressure

S33 < 60% pressure

If both pumps were to cavitate at the same time, the cause would probably be attributable to a common fuel-oxidizer pressurization failure. In this case the V = (S32) (S33) = 1 would not obtain. Another separation calling for engine shut down without restart would obtain, however. This would be the best choice in this instance, because the chance of restart is small if both pumps have cavitated due to low inlet pressures.

Following a similar line of reasoning, additional functionally redundant V equations for pump cavitation can be generated. For oxidizer or fuel pump cavitation some of the equations are:

(S11) $(\overline{S12})$	ox flow normal, fuel flow low
(S11) (S12)	ox flow low, fuel flow normal
(S32) $(\overline{S33})$	ox pressure normal, fuel pressure low
$(\overline{S32})$ (S33)	ox pressure low, fuel pressure normal
(S11) $(\overline{S33})$	ox flow normal, fuel pressure low

etc.

Note that any of the above equations may be "anded" with (S6), where binary one for S6 is greater than 90 percent speed, as before. This does not change the situation, because the limits chosen for the S11, S12, S32, S33 set would, in general, not be reached until the engine is at 90 percent speed. It is questionable whether "anding" the (S6) term is of any value in improving the overall V equation, however. It will certainly increase the missed alarm rate and is, therefore, omitted.

K-4. RELIABILITY OF V'S

All V equations are the result of analysis of the cause and effect relationships in the engine. The relationships between the V

equations and the malfunctions are, therefore, deterministic. Even when evaluating V equations where the occurrence of the signals is not known with certainty, the deterministic quality can be retained. For instance, a given failure area, m_x, may result in fire 50 percent of the time. To evaluate a fire detector with relation to m_x, the failure area is divided in two parts, m_{x1} which leads to fire and m_{x2} which does not.

The equipment, however, exhibits statistical failures which can cause false and missed alarms. These effects may be controlled by employing functional redundancy, component redundancy and self-check. The self-check provisions are described in Appendix E. The equipment designer is free to use various combinations of S's and V's to get the desired effect. Assume, for instance, that in using $V = 1 = (S32)(\overline{S33})$ a false alarm problem arises due to failures in the S33 sensor. An improvement would be achieved by suing two identical sensors for S33:

$$V = 1 = (S32)\ (\overline{S33})\ (\overline{S33}).$$

The full expected reduction in false alarms will not be realized, however, because there is undoubtedly a functional dependence between the failures in the S33 sensors, since they are identical devices operating in the same environment. If an (S12) flow signal is available, perhaps from another V expression, an alternate formulation could be used.

$$V = 1 = (S32)\ (\overline{S33})\ (\overline{S12})$$

The selection of the optimum redundant technique falls in the category of system evaluation treated in Appendix F.

This example goes somewhat beyond the basic problem of signal space separation design but serves to underline the close relationship between the design of V's and the subsequent design of equipment.

K-5. VARIATION OF STORED REFERENCES

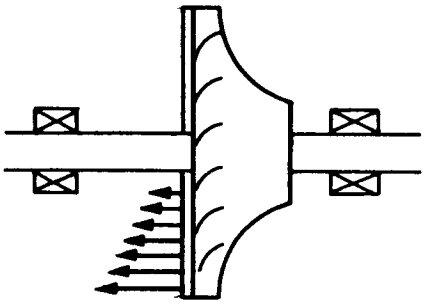
A typical comprehensive READI system will use a large number of stored references. The design described in Appendix E, for instance, uses 31 such references. Many of the reference values are constant, or nearly so, for all operating conditions. For instance, S31 - S32 = 10 psia;

the 10 psia reference does not change. However, it is necessary to adjust many of the references if the separations are to be made with the required accuracy and false alarms are to be eliminated. A typical variation of a reference appears in figure K-3, where the reference for S11, oxidizer flow as used in m3, low oxidizer flow, is shown to vary with engine O/F and thrust.

K-6. SPECIALIZED TECHNIQUES

All techniques mentioned so far are, to a degree, general in their application to liquid rocket engines. When dealing with a specific engine, the peculiarities in the machine suggest the development of highly specialized techniques. Several such techniques are noted here.

One of the methods used to minimize the axial load in large centrifugal pumps is to balance the load hydraulically. An axial force is developed by a pressure gradient, as shown in the accompanying sketch on the pump wheel so that only a small part of the axial load



must be carried by the bearings. Bearing and/or pressure balancing system failures may be detected by monitoring the balancing pressure. This signal is particularly valuable because it predicts failure in advance of occurrence.

A common method of reducing pipe flange leakage, as shown below, in cryogenic systems is to employ redundant or series gasket designs. When such an arrangement is employed the opportunity for detecting small leaks past the first gasket is presented. The sensor can detect the presence of the leaking medium in a number of ways. One of the simplest is to use a sensor containing a small heated

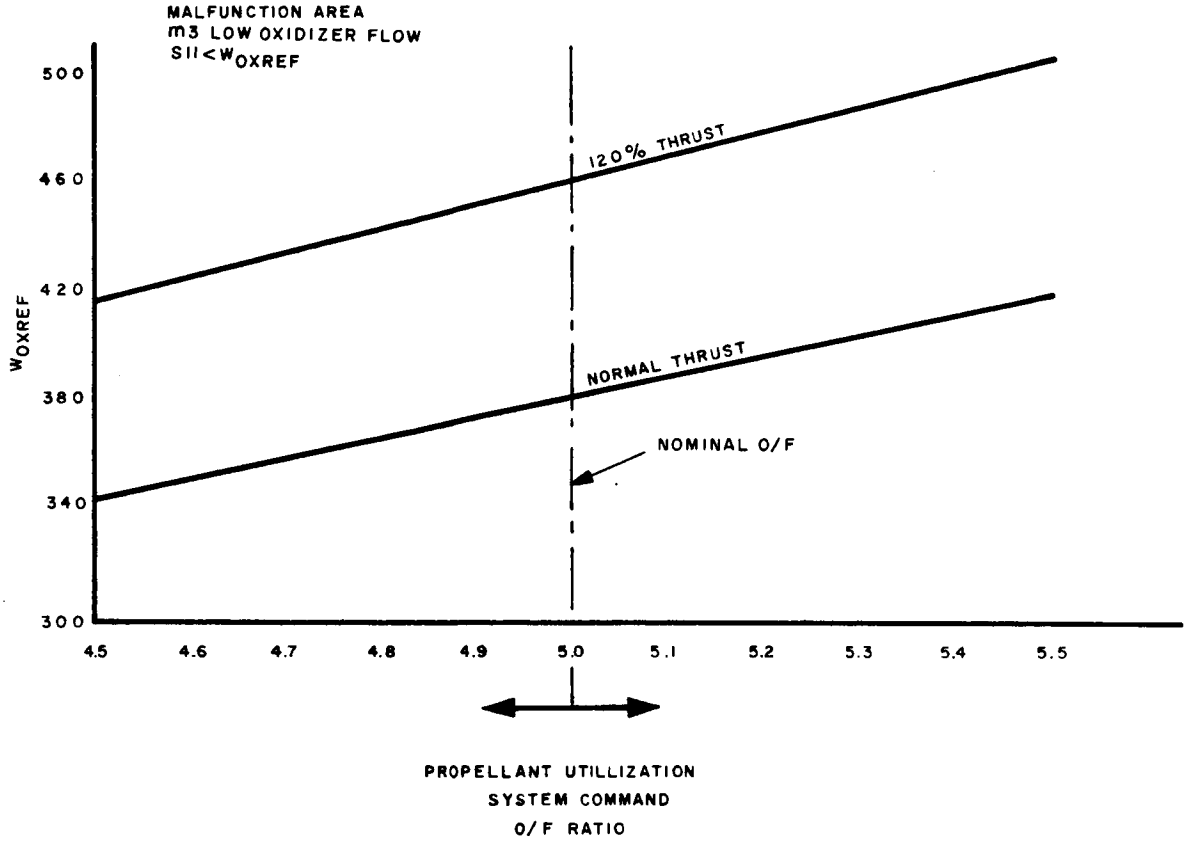
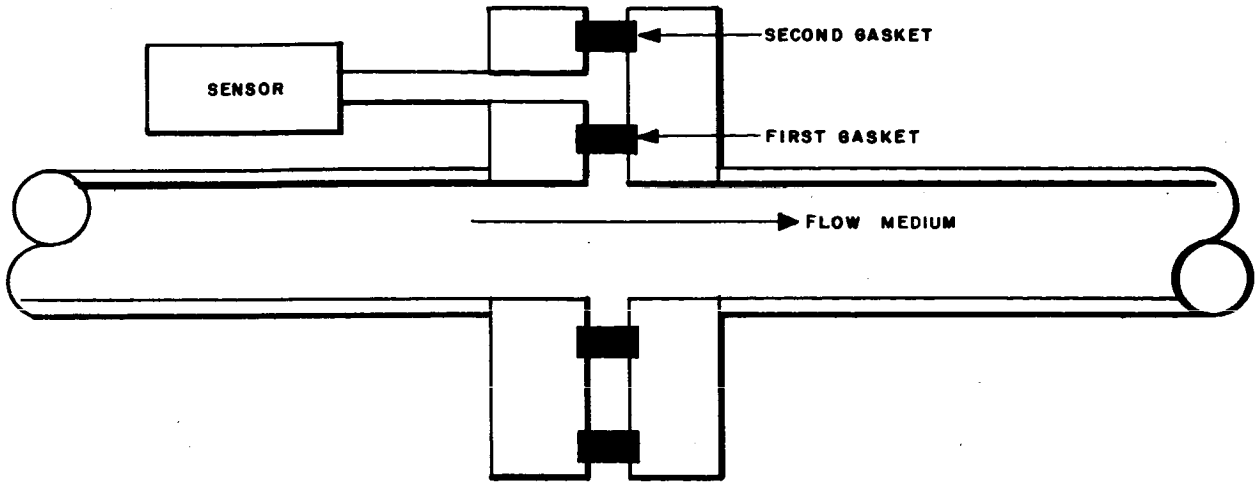


FIGURE K-3

VARIATION OF STORED REFERENCE WITH
O/F AND THRUST (TYPICAL)



thermopile which is cooled by the flow of the leaking medium. Such sensors can be designed to react to minute flows. However, an essential point is that the introduction of the sensor does not increase the leakage problem.

Another consideration in evaluating this sensing technique (and all others too) is, having detected the presence of a failure, in this case a small leak, what corrective step can be taken. If no corrective step can be taken, the measurement is not to be rejected immediately. The failure may later lead to a more serious condition. A confusion of failure signals may ensue, and the incipient leak measurement could be the deciding factor in selecting among the alternates of engine shutdown, increasing thrust, or signaling abort.

A signal indicating a small leak will be of more concern in the second stage, before rather than after second stage separation, because the engine area is generally enclosed in a boat tail or skirt before separation. Little or no fire hazard, due to fuel leaks alone, exists following separation. Therefore, time-to-separation is a vital factor in formulating a signal space separation using the subject leak signal.

K-7. PREDICTIVE TECHNIQUES IN SIGNAL SPACE SEPARATION

Many of the common techniques of engine condition identification are predictive in nature. The use of a turbine acceleration limit for instance is a method of predicting, and forestalling, failure of the turbine wheel. The following paragraphs discuss some of the further possibilities of predictive technique as applied to decision logic and displays.

A. APPLICATION TO DECISION LOGIC

One fundamental type of prediction is a linear extrapolation of the variable to determine if a limit will be exceeded.

$$x(t) + \frac{dx}{dt} (\text{time to go}) > \text{limit}$$

For instance, the turbine acceleration limit is implemented in the following manner:

$$K_1 (S6) + K_2 (S54) > \text{limit}$$

where

S6 = speed signal

S54 = $\frac{d(S6)}{dt}$ acceleration signal

K15 = constants

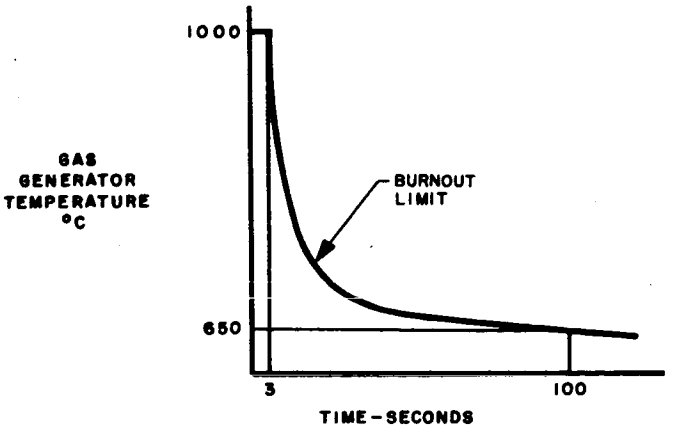
This equation simply states that the speed is above 27,000 rpm and increasing at 40,000 rpm/sec. The "time-to-go" term, which is stage time-to-burn, does not come into play because, for this V equation, the limit would be exceeded for all values of time-to-go up to the last second of burning.

Three additional examples of the use of predictive techniques will be considered. They are:

- Gas generator temperature
- Thrust chamber O/F ratio
- Propellant tank pressure.

B. GAS GENERATOR TEMPERATURE

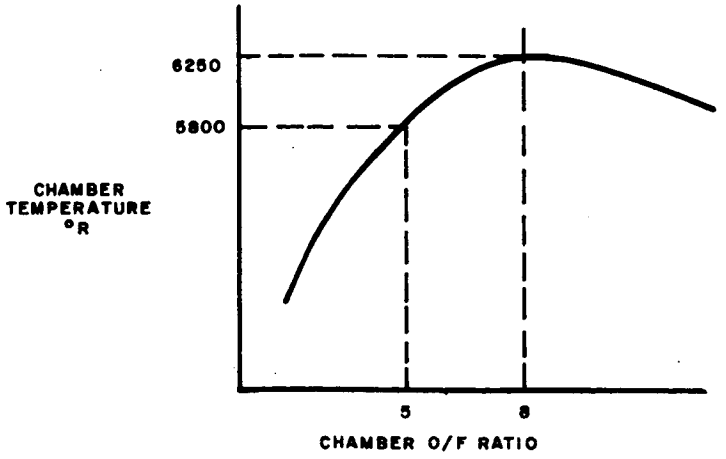
Gas generator temperature rate is of value in predicting turbine burnout and overspeed. The burnout limit is itself time and temperature dependent as shown below.



The limit is, therefore, roughly the integral of the time and temperature in excess of the asymptotic temperature. For a typical turbine like the one shown, the limit is about 1000 degree (C)-seconds.

C. THRUST CHAMBER O/F RATIO

Thrust chamber O/F is the primary variable in determining combustion temperature. The following figure shows the chamber temperature for the READI model engine for 600 psia chamber pressure. The rise in temperature from an O/F of 5:1 to 8:1 may or may not cause chamber failure depending on the chamber design (and safety margin) and the failure which caused the rise in O/F. For instance, high chamber O/F can result from fuel leakage or from oxidizer injector erosion. Since fuel leakage reduces heat transfer (fuel is the cooling medium), the likelihood of chamber failure is much higher with a severe fuel leak than with oxygen injector erosion.



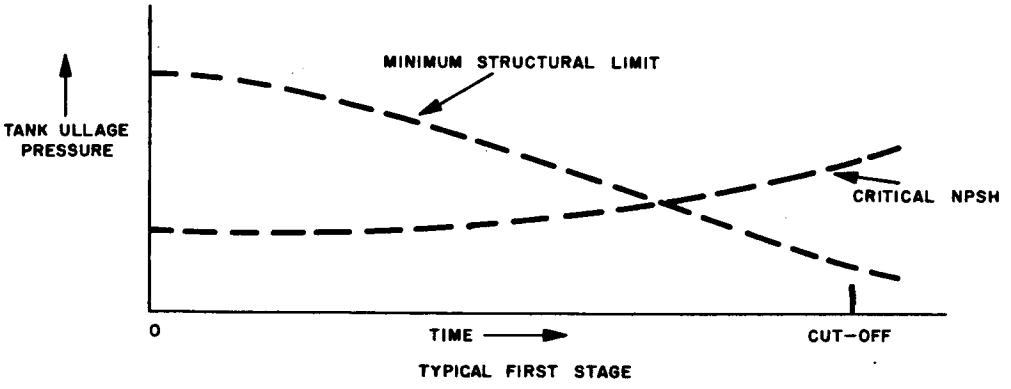
As the O/F increases beyond 8:1, the temperature drops, but the problem gets worse because the mixture is becoming more and more oxidizing in nature, and chamber burnout will occur if a corrective measure is not taken. As with gas generator temperature, the chamber temperature (that is, O/F) anticipates the failure.

D. PROPELLANT TANK PRESSURE

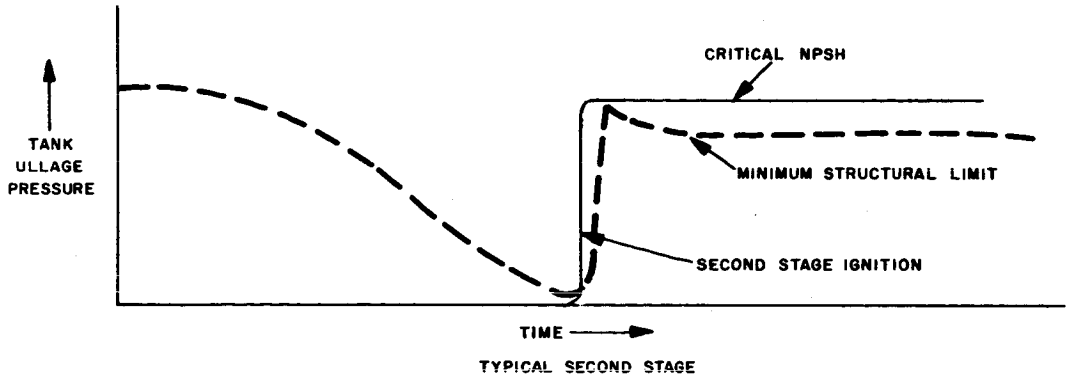
There are generally two limits which must be considered in looking at propellant tank pressure:

- The critical net position suction head, NPSH, required by the engines, which is in the 35 psia region for the READI model engine.
- The minimum structural threshold of the stage with thrust, if the tanks depend upon internal pressure to any degree.

Both of these limits can be time dependent depending on whether one is considering the first or second stage and on the design of the tanks. For the first stage the structural threshold generally decreases with time, and the critical NPSH may increase slightly. In the second stage the time variation is less because the vehicle is out of the atmosphere. (See accompanying sketches.)

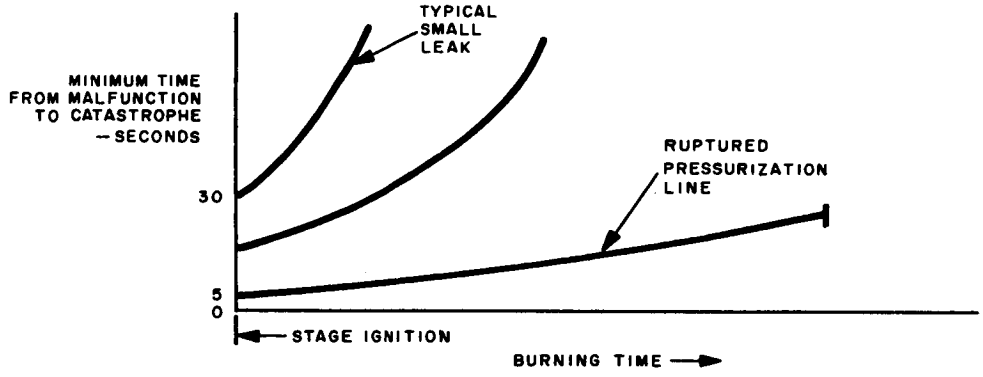


TYPICAL FIRST STAGE



TYPICAL SECOND STAGE

The required reaction time for a READI system is related to the time to catastrophe. In the case of large tank or line leaks the corrective action is to abort, the objective being to do so before the vehicle collapses. Typical required reaction times are shown in the following sketch.



K-8. ENGINE-TO-ENGINE COMPARISON

One of the problems which arises in attempting to identify the condition of the engine is finding suitable reference values and/or gate signals. In some cases (m16, 17, 18), it is necessary to store in READI the malfunction response limits in the form of multi-dimensional functions. In addition, other normally fixed limits change when the engine thrust and/or O/F ratio changes. A possible solution for some malfunctions is simply to reference the subject engine to the others. In a cluster of engines which are nearly

identical, one engine is an excellent analog of another. Even during transients, normally functioning engines track each other with good fidelity. [1]

The possible advantages which can be listed for this approach are that it:

- eliminates the need for stored references
- reflects effect of changes in command thrust and O/F
- reflects effects of changes in engine propellant inlet temperature and pressure
- compensates for unpredictable effects on all engines
- eliminates most of the "gating" signal requirements
- can be made to work better than stored reference systems during engine acceleration to main stage operation.

Possible disadvantages of this approach are that it:

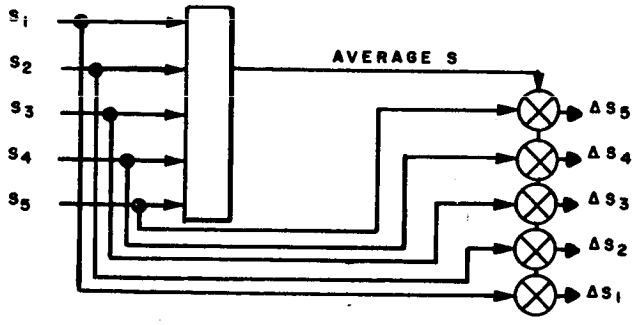
- won't work on single engine stages, a new design using stored references being required
- presents a problem in development program; it would be necessary to develop a dynamic signal generator to simulate other engines to permit single engine-analyzer testing.

- - - - - - - -

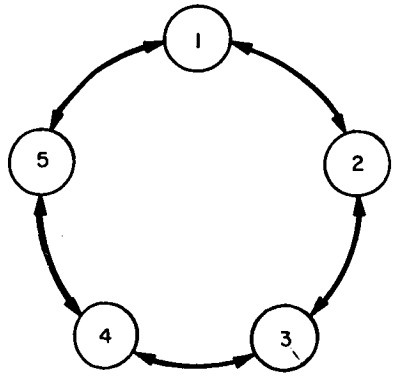
[1] Typical starting transient data for time from fire switch to 90-percent chamber pressure are noted below, where all figures are in milliseconds:

	Mean	Engine-to-Engine Sigma	Run-to-Run Sigma
Typical LO_2 - RR1 Engine	971	87	83
Typical LO_2 - LH_2 Engine	1554	-	131

There are several ways to implement engine-to-engine comparison. One of the obvious approaches to average all of the signals and then compare the individual signals to the average, as shown below. The comparison can be accomplished on a continuous basis or at quantized levels. Since a discrete decision is to be invoked, the latter is a more likely method.



Another approach is to compare the subject engine with only two others. For instance, as shown in the accompanying sketch, No. 3 engine is compared to No. 2 and 4.



The comparisons then boil down to a process of subtracting the signals from engine-to-engine, that is, $(S_1 - S_2)$, $(S_2 - S_3)$, etc. As an example, an engine-to-engine signal space separation has been written for m_2, low fuel flow to chamber.

m_2 Low Fuel Flow

S12 Fuel flowmeter

$(S12_1, S12_2, S12_3, S12_4, S12_5)$

Definition for binary one

$(S12_1 - S12_2) > |6|$ lb/sec
$(S12_2 - S12_3) > |6|$ lb/sec
$(S12_3 - S12_4) > |6|$ lb/sec
$(S12_4 - S12_5) > |6|$ lb/sec
$(S12_5 - S12_1) > |6|$ lb/sec

S31 Fuel pump inlet pressure

$(S31_1, S31_2, S31_3, S31_4, S31_5)$

Definition for binary one

$(S31_1 - S31_2) > |10|$ psi
$(S31_2 - S31_3) > |10|$ psi
$(S31_3 - S31_4) > |10|$ psi
$(S31_4 - S31_5) > |10|$ psi
$(S31_5 - S31_1) > |10|$ psi

$$A \begin{cases} (S12_1 - S12_2)(S12_5 - S12_1) \\ (S12_2 - S12_3)(S12_1 - S12_2) \\ (S12_3 - S12_4)(S12_2 - S12_3) \\ (S12_4 - S12_5)(S12_3 - S12_4) \\ (S12_5 - S12_1)(S12_4 - S12_5) \end{cases} \quad B \begin{cases} (S31_1 - S31_2)(S31_5 - S31_1) \\ (S31_2 - S31_3)(S31_1 - S31_2) \\ (S31_3 - S31_4)(S31_2 - S31_3) \\ (S31_4 - S31_5)(S31_3 - S31_4) \\ (S31_5 - S31_1)(S31_4 - S31_5) \end{cases}$$

(A + B) Final Boolean equation for low fuel flow.

Although the array of equations looks rather formidable, it must be noted that the above listing represents the processing for five engines.

There are also some subtile advantages to the use of the above equations. The pressure difference signals, $S31_1 - S31_2$, for instance, can be obtained by connecting a differential pressure sensor from one engine to the next, thus simplifying the processing and minimizing the effect of transducer inaccuracy. It may be possible to use raw flow data from the volumetric engine flowmeters since, under normal conditions, the engine-to-engine variation in fuel pressure and temperature will be small.

This technique, therefore, shows promise especially in dealing with some of the more complex signal space separations and in cases where transducer inaccuracy is a problem.

K-9. SIGNAL SPACE SEPARATION DOCUMENTATION

A standard format has been evolved for documenting the necessary information for evaluation of V equations and for the subsequent design of equipment. A sample of the form is shown in figure K-4. All of the processing required from input signal to decision logic is shown. Also, the decisions, reaction times, and correction time logs are shown.

K-10. OPTIMUM SET POINT AND ACCURACY FOR VARIABLE AMPLITUDE MALFUNCTIONS

Half of the malfunction areas in the model engine fall in a category of discrete occurrences, such as failure of valves to open or close. For discrete failures the problem of establishing a set point is simple because signals can generally be found which depart from normal by a large degree when the failure occurs. For the same reason sensor accuracy is usually not a problem.

Malfunctions such as injector erosion, burnout, leaks, and failures in the gas generator and turbopump however generally have a variable amplitude probability distribution, where the probability of occurence decreases with severity. For example, a typical engine is likely to have more small propellant leaks than large ones. The question which arises is "at what amplitude does one define the condition as being a malfunction and take corrective action, and what accuracy of signal separation is needed?"

This paragraph describes an analytical method which yields the optimum transducer set point and shows the effect of transducer accuracy on system effectiveness. The unit of comparison is reduction in risk from no READI to the same condition with READI. The effect of READI failures is not included in this method since it is treated elsewhere in the design procedure.

A. ANALYTICAL PROCEDURE

The difference in risk, ΔR_t, for two systems without and with READI for one malfunction is given by the following equations:

$$\text{Risk, no READI} = \int P(\omega)\ R_o(\omega)\ d\omega$$

$$\text{Risk, with READI} = \int \left[P(\omega)\ S_1(\omega)\ R_1(\omega) + P(\omega)\ [1 - S_1(\omega)]\ R_o(\omega) \right] d\omega$$

where

$P(\omega)$ = malfunction amplitude (magnitude) probability

$S_1(\omega)$ = probability of sensing malfunction. With a perfectly reliable system this is the same as the probability of taking the correct action.

$R_o(\omega)$ = risk as a function of ω (in this case the risk associated with turbine wheel strength) with no remedial action taken for malfunction

$R_1(\omega)$ = risk as a function of ω with remedial action taken for malfunction

If ΔR_t is defined as the risk without READI minus the risk with READI,

$$\Delta R_t = \int P(\omega)\, S_1(\omega)\, [R_o(\omega) - R_1(\omega)]\, d\omega$$

In order to evaluate the effect of set point and accuracy it is necessary to formulate models for $P(\omega)$, $S_1(\omega)$, $R_o(\omega)$ and $R_1(\omega)$.

1. Malfunction Amplitude Model

The top graph in figure K-5 shows an assumed malfunction amplitude model where the magnitude of malfunction is taken as the degree of overspeed of a turbine above the normal 100 percent level. Since normal operation is the dominant state of the system, the $P(\omega)$ has a very large value around 100 percent speed, as shown by the near vertical asymptote at 102 percent speed. Starting transients and other tolerable effects can cause speed variations up to about 120 percent speed. Above 120 percent speed a malfunction is assumed to have occured as shown by the shaded area. This assumption, however, does not play a part in the analysis. A linear distribution was drawn from 102 percent speed to 150 percent, the maximum expected speed. The total area under the curve is one.

2. Risk Model

The second curve in figure K-5 shows the risk with and without action versus the magnitude of failure in percent speed. The no action $R_o(\omega)$ risk will be recognized as one of the curves calculated

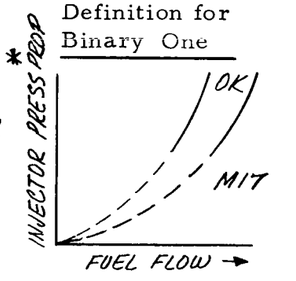
Stage 2
Engine
Number M17

Signal Space Separation

EXCESS FUEL FLOW TO MAIN CHAMBER

Group PROPORTIONAL, COMBINATION LOGIC
Operational Modes When Used
Inputs

Code	Source Designation	t_t (ms.)	Definition for Binary One
S12	FUEL FLOW (FM1)		
S25	FUEL INJECTOR PRESSURE PROP } MAIN		
S55	FUEL INJECTOR TEMPERATURE } CHAMBER		



* CORRECTED FOR TEMP.

Processing (FOR BINARY ONE)
$S25 + \epsilon < (2+0.01 S55) S12 - 220$
ϵ = ACCEPTABILITY LIMIT

Failure(s)

No.	Type	Final Effect	t_F (ms.)
1	CHAMBER LEAKAGE (EXTERNAL }	EXCESS FUEL CONSUMPTING	>1000
2	EXTERNAL LINE LEAKAGE }	OVERBOARD LOSS	
3	CHAMBER BURNOUT	EXCESS FUEL CONSUMPTION	>1000
		HIGH O/R, PROGRESSIVE FAILURE - ENGINE DESTRUCTION	

Corrective Action(s)

No.	Action	t_c (ms.)
1	MALFUNCTION SHUTDOWN	300
2	INCREASE THRUST ON OTHER ENGINES	100

*See Detailed Discussion

READI FORM NO. 1

Stage 2
Engine
Number M7

Signal Space Separation

NO PUMP SPEED

Group BINARY COMBINATION LOGIC
Operational Modes When Used OPERATION (MAINSTAGE)
Inputs

Code	Source Designation	t_t (ms.)	Definition for Binary One
S3	FIRE VOLTAGE		
S21	TURBOPUMP SHUT-OFF VALVE (U6) LIMIT SW.		U6 OPEN
S51	GG FUEL INJECTOR PRESSURE		> 200 PSIA
S33	FUEL PUMP DISCHARGE PRESSURE		> 830 PSIA
S6	TURBINE SPEED		> 40%
S52	1½ SEC. DELAY FROM S3		

Processing (a) $(\overline{S3})(\overline{S6})(\overline{S52})$
(b) $(\overline{S3})(\overline{S21})$
(c) $(\overline{S3})(\overline{S33})(\overline{S51})$

Failure(s)

No.	Type	Final Effect	t_F (ms.)
1	TURBOPUMP SHUT-OFF VALVE (U6) FAILED CLOSED	NO THRUST	>1000
2	TPSO PILOT VALVE (U10) FAILED CLOSED	" "	>1000
3	TURBOPUMP GEAR/BEARING FAILURE	" "	>1000
4	TURBOPUMP STRUCTURAL FAILURE	" "	*
5	GG RUPTURE	" " (FIRE HAZARD)	≈ 1000

Corrective Action(s)

No.	Action	t_c (ms.)
1	MALFUNCTION SHUTDOWN	~ 300
2	INCREASE THRUST ON OTHER ENGINES	~ 100

*See Detailed Discussion

READI FORM NO. 1

FIGURE K-4
SAMPLE SIGNAL SPACE SEPARATION

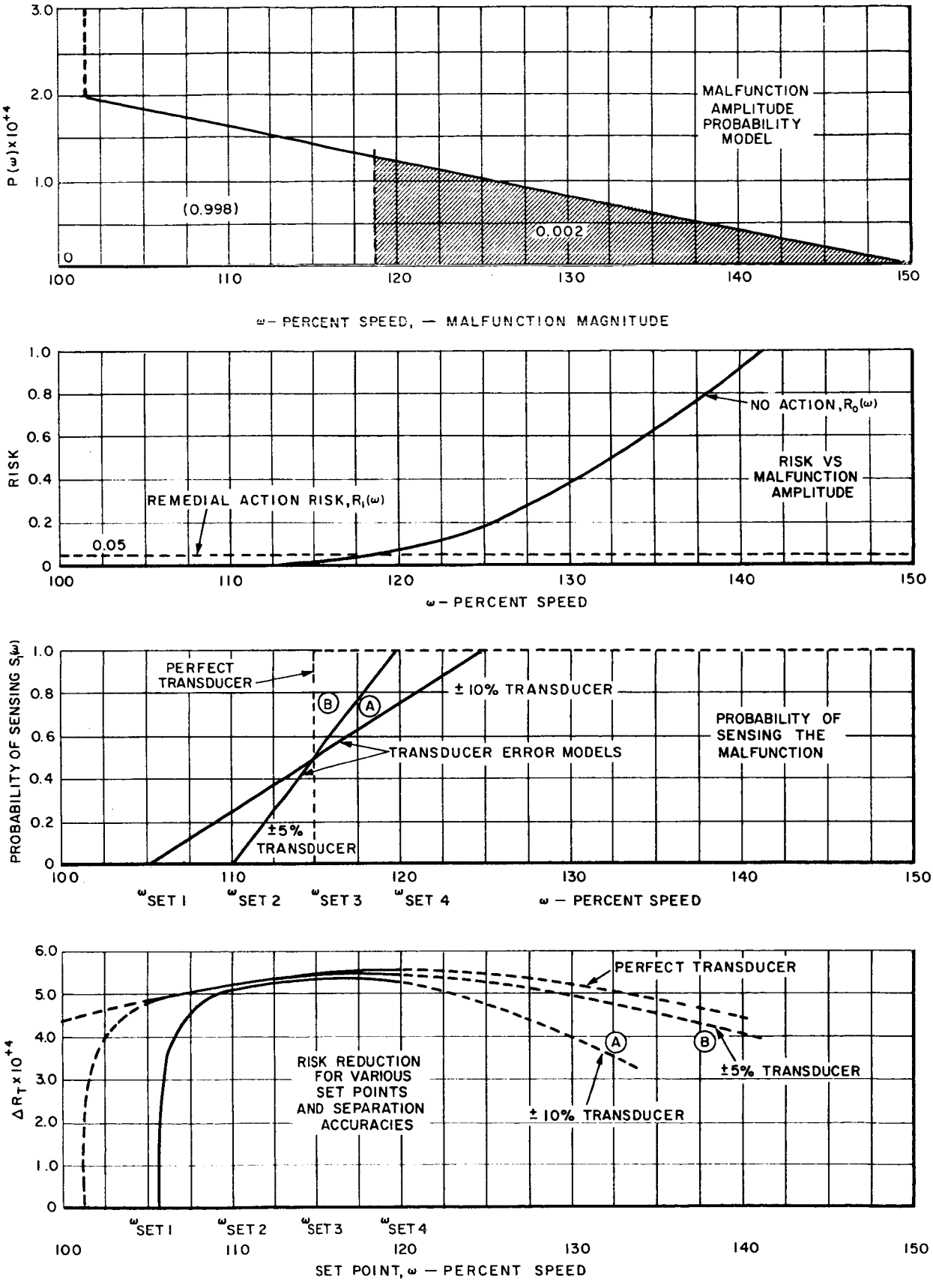


FIGURE K-5 ACCURACY - SET POINT TRADE OFF FOR VARIABLE AMPLITUDE MALFUNCTIONS

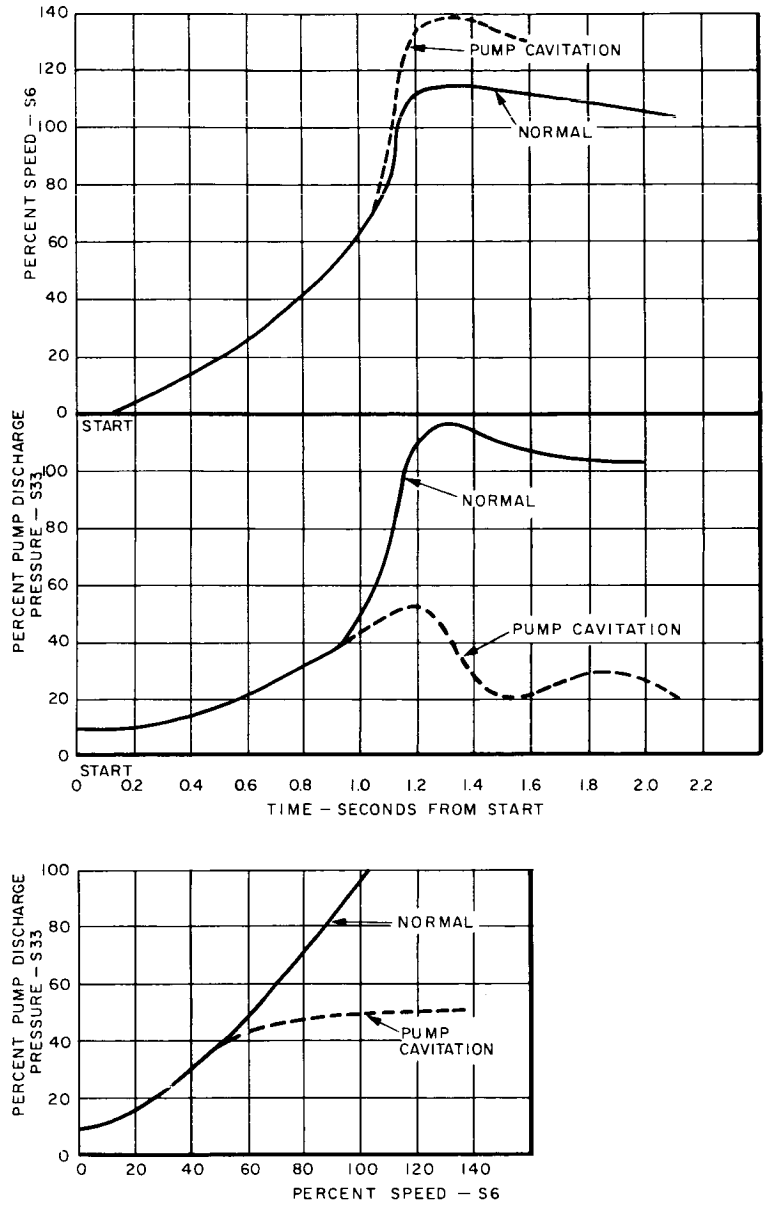


FIGURE K-6 TYPICAL STARTING TRANSIENTS WITH AND WITHOUT PUMP CAVITATION

in Appendix J for turbine wheel strength. The causes of the over speed condition include high gas generator O/F, premature main propellant valve and tank safety valve closure, and pump cavitation. The maximum risk is set at 1.0, and the remedial action risk, $R_1(\omega)$, at 0.05. For the READI model engine the maximum risks (i.e. loss x probability of one) for the failures noted range from 1.3 to 6.1.

3. Sensor Model

The third curve in figure K-5 shows three models for the probability of sensing the overspeed condition, a perfect transducer and two real transducers with total error bands of ±5 percent and ±10 percent. A straight line approximation to the integral of the transducer error distribution is used. Various set points are achieved by moving the S(1) curve along the ω axis.

The maximum reduction in risk, ΔR_t, may be found by differentiating the ΔR_t equation and setting the result equal to zero.

$$P(\omega)\, S_1(\omega)\, [\, R_o(\omega) - R_1(\omega)\,] = 0$$

$P(\omega)$ will produce a minimum above 150 percent speed and S(1) will produce a minimum below the break point in the S(1) vs. ω model. The maximum ΔR_t will occur at the point where $R_o(\omega) = R_1(\omega)$.

B. CONCLUDING REMARKS

The best set point occurs where the risks with and without correction action are equal. The ±10 percent transducer is adequate for the models used in this example, but it is apparent that the accuracy effect is quite sensitive to the shape of the probability and risk models. A more accurate transducer would be required if the $P(\omega)$ curve had a higher slope between 102 and 150 percent speed or if the R(o) curve were to rise more sharply in the range where it crosses the R(1) curve.

The procedure described here offers a method of arriving at an acceptable trade-off of accuracy of separation and set point as a function of risk-reduction for variable amplitude malfunctions. At the least, when information is lacking to perform the calculations, the procedure identifies the areas of information required, i.e., the risk model, malfunction amplitude model, and transducer accuracy model.